Memorandum of Understanding between the Regulation and Quality Improvement Authority and the Health & Care Professions Council

April 2022

Memorandum of Understanding between the Regulation and Quality Improvement Authority and the Health & Care Professions Council

Introduction

1. The purpose of this Memorandum of Understanding (MoU) is to set out a framework to support the working relationship between the **Regulation and Quality Improvement Authority (RQIA)** and **the Health & Care Professions Council (HCPC)**.

2. The working relationship between the RQIA and HCPC is an important element of an effective regulatory system for health and social care in Northern Ireland.

3. RQIA is the regulator of health and social care in Northern Ireland. The HCPC is the independent regulator for allied health professionals. The responsibilities and functions of the RQIA and HCPC are set out at Annexe A.

4. This MoU does not override the statutory responsibilities and functions of the RQIA or HCPC and is not enforceable in law. However, the RQIA and HCPC are committed to working in ways that are consistent with the contents of this MoU.

Principles of cooperation

5. The RQIA and HCPC intend that their working relationship will be characterised by the following principles:

    - The need to make decisions which promote people's safety and high quality health and social care.
    - The need to build and maintain public and professional trust and confidence in the two organisations.
    - Openness and transparency between the two organisations, as to when cooperation is and is not considered necessary or appropriate.
    - The need to use resources effectively and efficiently.
    - A commitment to address any identified overlaps or gaps in the regulatory framework and responsibilities.
    - Respect for each organisation's independent status.

6. The RQIA and HCPC are also committed to a regulatory system for health and social care in Northern Ireland, which is transparent, accountable, proportionate, consistent, and targeted - the principles of better regulation.

Areas of cooperation

7. The working relationship between the RQIA and HCPC involves cooperation in the areas detailed in paragraphs 8-17. Named MoU leads for each organisation are identified at Annexe B.

Cross-referral of concerns

8. Where the RQIA or HCPC encounters a concern which it believes falls within the remit of the other organisation, they will at the earliest opportunity convey the concern and relevant information to a named individual with relevant responsibility at the other organisation. Named leads are identified in Annexe B. The referring organisation will not wait until its own investigation has concluded.

9. In particular, RQIA may refer to the HCPC:

    - Any concerns and relevant information about an allied health professional which may call into question their fitness to practise.
    - Any concerns and relevant information about a healthcare organisation or a part of that organisation which may call into question its suitability as a learning environment for allied health professional students.
    - Any concerns and relevant information relating to the general delivery of allied health professional care at a health or social care organisation which may call into question issues of allied health professional leadership.
    - Any information about an individual purporting to be an allied health professional where RQIA has reason to believe that the person is not on the HCPC register.
    - Any thematic issues about an allied health professional that could be addressed through setting professional standards.

10. In particular, the HCPC may refer to RQIA:

    - Any concerns and relevant information which may be useful intelligence about a healthcare or social care organisation or regulated service, in which allied health professionals practise.
    - Any concerns and relevant information which may be useful intelligence about a healthcare or social care organisation where student allied health professionals are trained which may call into question the quality and services it provides or its registration with the RQIA.

Exchange of information

11. Cooperation between the RQIA and HCPC will often require the exchange of information. All exchanges of information will be lawful, proportionate and shared with the named contact in the other organisation at the earliest possible opportunity.

12. All arrangements for collaboration and exchange of information set out in this MoU and any supplementary agreements will take account of and comply with Annexe C (Data Protection) to this MoU, the Data Protection Act 2018, UK General Data Protection Regulation, the Freedom of Information Act 2000 and any RQIA and HCPC codes of practice, frameworks or other policies relating to confidential personal information.

13. Exchange of information will be expected, but not limited, to cases:

    - outlined in paragraphs 9 and 10 in this MoU
    - where a resolution to a concern would benefit from a coordinated multi-agency response.

14. Both the RQIA and HCPC are subject to the Freedom of Information Act 2000. If one organisation receives a request for information that originated from the other, the receiving organisation will make the other aware before responding.

Media and publication

15. RQIA and the HCPC will endeavour to give each other at least 24 hours warning of, and sufficient information about, any planned public announcements on issues relevant to the other organisation, including the sharing of draft proposals and publications where specific concerns are identified. It is acknowledged that this may be challenging in some circumstances, such as where urgent enforcement action is required.

16. RQIA and the HCPC respect the confidentiality of any documents shared in advance of publication and will not act in any way that would cause the content of those documents to be made public ahead of the planned publication date.

17. RQIA and the HCPC may work together, where appropriate, to produce joint statements or communications highlighting collaboration or activities relevant to both organisations where specific concerns are identified.

Resolution of disagreement

18. Any disagreement between RQIA and the HCPC will normally be resolved at working level. If this is not possible, it may be brought to the attention of the MoU leads identified at Annexe B who may then refer it upwards through those responsible, up to and including the Chief Executives of the two organisations who will then jointly be responsible for ensuring a mutually satisfactory resolution.

Duration and review of this MoU

19. This MoU is not time-limited and will continue to have effect unless the principles described need to be altered or cease to be relevant. The MoU will be reviewed by the MOU managers annually but may be reviewed more urgently at any time at the request of either organisation. Changes to the MoU will however require both parties to agree, with the exception of contact details which may be changed unilaterally.

20. Both RQIA and the HCPC are committed to exploring ways to develop increasingly more effective and efficient partnership working to promote quality and safety within their respective regulatory remits. The effectiveness of the working relationship between RQIA and the HCPC will be supported by regular contact, either formally or informally. Meetings to discuss intelligence, policy and operational issues of interest to both organisations should take place between relevant colleagues at both organisations when appropriate.

21. Both organisations have identified a MoU manager at Annexe B and these will liaise as required to ensure this MoU is kept up to date and to identify any emerging issues in the working relationship between the two organisations.

Signed:

Briege Donaghy
Chief Executive
Regulation and Quality Improvement Authority

Date: 27/04/2022

Mr John Barwick
Chief Executive and Registrar
Health & Care Professions Council

Date:04/04/2022

Annexe A: Responsibilities and functions

1. The Regulation and Quality Improvement Authority (RQIA) and the Health & Care Professions Council (HCPC) acknowledge the responsibilities and functions of each other and will take account of these when working together.

Responsibilities and functions of RQIA

2. Regulation and Quality Improvement Authority

RQIA is an independent body established by the Department of Health and Social Services and Public Safety in April 2005, under the Health and Personal Social Services (Quality, Improvement and Regulation) Order (2003 NI) (The Order (2003)).

- Under the provision of The Order (2003) the RQIA is required to keep the department informed about the provision, availability and quality or services; and also encourage improvement in the delivery of services.

- RQIA has powers to conduct reviews and carry out investigations/inspections into the management, provision, quality of or access to and availability of HSC services; including clinical and social care governance arrangements.

- Any person who carries on or manages an establishment or agency must make an application to RQIA to register. Once granted, RQIA issues a certificate of registration to the applicant. RQIA maintains a register of all approved establishments and Agencies.

- Under the Mental Health Order (1986 NI) and from 1 October 2019, the Mental Capacity Act, 2016, RQIA undertakes a range of responsibilities for people with a mental illness and those with a learning disability.

- RQIA is designated as a National Preventative Mechanism (NPM) under the Optional Protocol to the Convention against Torture and other Cruel, Inhumane or Degrading Treatment or Punishment (OPCAT); an international human rights treaty designed to strengthen protection for people deprived of their liberty. OPCAT requires NPMs to carry out visits to places of detention to monitor the treatment of and conditions for detainees and to make recommendations regarding the prevention of ill-treatment. All NPMs report to and work towards guidance and reports issued by the UN Subcommittee on Prevention of Torture and Other Cruel, Inhuman or Degrading treatment or Punishment.

- The RQIA has four core values that underpin their work. In all that they do they will be FAIR – fair and accountable, and act with integrity and respect. RQIA has adopted the regional health and social care values. Which are:

    - Working together

- Excellence
- Compassion
- Openness and honesty

Responsibilities and functions of the HCPC

3. The Health and Care Professions Council is the regulator of 15 professions:
   Arts therapists
   Biomedical scientists
   Chiropodists/ podiatrists
   Clinical scientists
   Dietitians
   Hearing aid dispensers
   Occupational therapists
   Operating department practitioners
   Orthoptists
   Paramedics
   Physiotherapists
   Prosthetists / Orthotists
   Practitioner psychologists
   Radiographers
   Speech& language therapists

4. The responsibilities and functions of the HCPC are set out in the Health Professions Order 2001 (the 2001 Order). The 2001 Order protects one or more designated titles for each of the relevant professions and anyone using one of those titles must be registered with the HCPC. Misuse of a title is a criminal offence.

5. Under the 2001 Order the principal functions of the HCPC are to establish standards of education, training, conduct and performance for members of the relevant professions and to ensure the maintenance of those standards. It does this by:

   - setting standards, including Standards of Proficiency, Standards of Conduct, Performance and Ethics and Standards of Education and Training;

   - approving education programmes and qualifications which meets its standards;

   - maintaining a register of appropriately qualified professionals; and

   - investigating and adjudicating complaints about their fitness to practise.

6. The over-arching objective of the HCPC in exercising its functions shall be the protection of the public.

7. The HCPC also has a duty to co-operate, with, among others, bodies concerned with the regulation of, or the co-ordination of the regulation of, other health and social care professionals, the regulation of health services, and the provision, supervision or management of health or education services.

Annexe B: Contact details

The Regulation and Quality Improvement Authority 9th Floor Riverside Tower 7th Floor Victoria House 15-27 Gloucester Street Belfast BT1 4LS	**Health & Care Council** 184-186 Kennington Park Road London SE11 4BU
Chief Executives *Internal escalating policies should be followed before referral to Chief Executives*	
Briege Donaghy Interim Chief Executive RQIA Briege.Donaghy@rqia.org.uk	John Barwick Chief Executive HCPC john.barwick@hcpc-uk.org
MOU management	
Jacqui Murphy Head of Business Services Unit Jacqui.murphy@rqia.org.uk	Claire Amor Head of Governance (DPO) Claire.amor@hcpc-uk.org
Operational	
Dr Julie-Ann Walkden Assistant Director of Reviews, Audit, Governance and Improvement Julie-Ann.Walkden@rqia.org.uk	Laura Coffey Head of FTP Laura.coffey@hcpc-uk.org
Communications	
Malachy Finnegan Communications Manager Malachy.Finnegan@rqia.org.uk	Tony Glazier Communications & Digital Lead Tony.glazier@hcpc-uk.org
DPA and FoI requests	
Hayley Barrett Business Manager Hayley.barrett@rqia.org.uk	As MOU Management

Annexe C: Data Protection

1. The following definitions apply in this Annexe C:

   1.1 **Agreed Purposes**: to allow the parties to comply with their statutory responsibilities and functions, to facilitate the co-operation of the parties pursuant to this MoU and any other purposes set out in the Data Access Agreement.

   1.2 **Controller, processor, data subject, personal data, personal data breach, processing and appropriate technical and organisational measures**: as set out in the Data Protection Legislation.

   1.3 **Data Access Agreement**: the data access agreement entered into between the RQIA and HCPC on or around the date of this MoU.

   1.4 **Data Discloser**: a party that discloses Shared Personal Data to the other party.

   1.5 **Data Protection Legislation**: all applicable data protection and privacy legislation in force from time to time in the UK including the Data Protection Act 2018 (**DPA 2018**) (and regulations made thereunder); the UK GDPR (which has meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data.

   1.6 **Permitted Recipients**: the parties to this MoU, the employees of each party, any third parties engaged to perform obligations in connection with this MoU, the Professional Standards Authority, any third parties attending hearings organised by the parties in connection with the Agreed Purposes and any third parties who may need to receive the Shared Personal Data for the Agreed Purposes.

   1.7 **Shared Personal Data**: the personal data to be shared between the parties under this Annexe C. Shared Personal Data shall be confined to the categories of information and categories of data subject as set out in the Data Access Agreement.

2. This Annexe C sets out the framework for the sharing of personal data between the parties as controllers. Each party acknowledges that one party (referred to in this Annexe C as the **Data Discloser**) will disclose, or allow access, to the other party Shared Personal Data collected by the Data Discloser for the Agreed Purposes. The lawful bases for sharing the Shared Personal Data are as set out in the Data Access Agreement. Each party shall comply with all the obligations imposed on a controller under the Data Protection Legislation.

3. Each party shall:

3.1 ensure that it has all necessary notices and consents and lawful bases in place to enable lawful transfer of the Shared Personal Data to the Permitted Recipients for the Agreed Purposes;

3.2 ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

3.3 process the Shared Personal Data only for the Agreed Purposes;

3.4 not disclose or allow access to the Shared Personal Data to anyone other than the Permitted Recipients; and

3.5 not transfer any personal data received from the Data Discloser outside the EEA.

4. Each party shall assist the other in complying with all applicable requirements of the Data Protection Legislation. In particular, each party shall:

4.1 promptly inform the other party about the receipt of any data subject rights request;

4.2 provide the other party, at the cost of the other party, with reasonable assistance in responding to any request from a data subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, personal data breach notifications, data protection impact assessments and consultations with the Information Commissioner or other regulators;

4.3 notify the other party without undue delay on becoming aware of any breach of the Data Protection Legislation; and

4.4 maintain complete and accurate records and information to demonstrate its compliance with this Annexe C.

Annexe D: data access agreement

Internal Ref. No.:
_____

DATA ACCESS AGREEMENT

IT IS IMPORTANT THAT YOU READ THIS SECTION BEFORE COMPLETING THE DATA ACCESS AGREEMENT (DAA) FORM

This Data Access Agreement (DAA) template should be completed ONLY where personal identifiable data is to be shared for a secondary purpose.

'Identifiable' means data which could lead to any individual being identified and includes pseudonymised data. (See Section A). A secondary purpose is a reason other than the initial purpose for which the data was collected

A DAA is NOT appropriate for the following purposes:

- When only anonymous (non-identifiable) data is to be shared
- Where identifiable data is to be shared for a primary purpose e.g. for a purpose linked to the direct care of the patient or service user; or a purpose linked directly to a staff member's employment. Contact your IG Department for further advice.
- Research (see below re Research Governance Framework)
- Software maintenance contracts (will be covered by the appropriate contract)
- Internal audits (seek advice from the Audit Department)
- Where a legally binding contract is more appropriate (e.g. with a 3rd party supplier)

When information is required for a secondary purpose other than those included above, it is important that you consider what type of data meets your requirements and that you complete section A before proceeding with this DAA.

Please note that the purpose of a DAA is only to address any data protection issues associated with the sharing of personal data. Any other issues regarding the availability or interpretation of data and arrangements or resources required to comply with the request should be discussed separately with the relevant Service / Information Dept. staff within the Trust(s).

Introduction

All Health and Social Care (HSC) organisations must ensure that when sharing HSC data for non-direct care (secondary purposes), assurances are provided by the requesting

organisations that they comply with data protection (DP) legislation and that staff are aware of the relevant DP policies and procedures in place.

Researchers undertaking studies and who require access to patient identifiable information and / or anonymous HSC data should follow the research protocol (Research Governance Framework for Health and Social Care in Northern Ireland). There is no need for an additional DAA to be completed.

Please be aware that it may be more appropriate to make use of the Honest Broker Service (HBS) rather than completing a Data Access Agreement. The HBS will enable the provision of anonymised, aggregated and in some cases pseudonymised health and social care data to the Department of Health (DoH), HSC organisations and in the case of anonymised data for approved Health and Social care related research.

Arrangement for access to personal data for a secondary purpose may already be covered by a contract (e.g. a contract for supplier support on an information system) therefore organisations need to be clear that any proposed data sharing is either covered adequately by that contract or make sure that a Data Access Agreement is completed.

The following Data Access Agreement must be completed and signed by any organisation wishing to access HSC identifiable data for a secondary purpose not already covered by a contract or research application. It must be considered for approval and signed by the owner organisation's Personal Data Guardian or Senior Information Risk Owner (SIRO).

In the event of a breach of this agreement which results in a financial penalty, claim or proceedings, the parties agree to co-operate to identify and apportion responsibility for the breach and the defaulting party will accept responsibility for any such claim.

Please refer to Appendix 2, 'Principles Governing Information Sharing' for guidance.

The form is divided into Sections (A-I) as detailed below:

Section A: Classification of data required
Section B: Title of Agreement / Details of Organisations to which the data will be shared
Section C: Details of Identifiable Data Items required and rationale
Section D: Consent or other Lawful Basis for accessing personal data
Section E: Data Protection arrangements (of receiving organisation)
Section F: Measures / Controls to prevent inappropriate disclosure of information
Section G: Data Retention
Section H: Declaration: Organisation to which data will be shared
Section I: Declaration: Owner Organisation

Appendix 1: Data Destruction Notification
Appendix 2: Principles Governing Information Sharing
Appendix 3: Definitions
Appendix 4: Contact Details

*****IMPORTANT*****

PLEASE REVIEW AND COMPLETE SECTION A BEFORE PROCEEDING

(A) Classification of data required (for secondary purpose)		
Identifiable data	The data to be shared with our organisation will contain Client Identifiable Details i.e. any of the following: Name, Address, Full Postcode, Date of Birth, HSC Number; Case-note Number; or other unique identifier that would link the data to identifiable details	Yes ☒ Please complete ALL sections of this DAA
Pseudonymous data	The data to be shared with our organisation contain no personal identifiers (as described above); however a unique code or key will be included that allows the possibility of linking this in future to a specific data subject. The pseudonymisation process will be completed at source by the HSC organisation who alone will securely retain the key to re-identify the data.	Yes ☐ Please complete sections B, C, and H of this DAA
Anonymous data	The data to be shared with our organisation will contain **NO** identifiable data items (as described above). At no stage will any party be able to link the data to an identified or identifiable natural person.	Yes ☐ A DAA is not required

When a DAA is appropriate, please ensure that the completed / signed form is returned to the relevant contact in each organisation (**see attached Appendix 4 for contact details**)

Please note that the completed Data Access Agreement will be immediately returned unless the receiving organisation has signed section H.

(B) Title of Agreement / Organisations to which the data will be shared

Title of Agreement	HCPC / RQIA MOU
Date of Request	April 2022

Please indicate as follows, by ticking the relevant box. This is:-

a) A New application ☐

b) Extending an earlier Agreement with no changes to what was previously agreed ☐

c) An update of an earlier Agreement with changes to what was previously agreed ☒

Please ensure that any changes from a previous agreement are clearly highlighted at Section C.

Date Access to Begin: ____April 2022_____

Date Access Ends: _____

2 yearly review date if on-going agreement:____ February 2024_____

Details of the Organisation the data will be shared with	
Name of Organisation: Health and Care Professions Council	
Name of Authorised Officer requesting Access to Trust Data	John Barwick
Position/Status	Chief Executive & Registrar
Address Postcode	Park House, 184/186 Kennington Park Road, London, SE11 4BU
Telephone Number	020 7840 9190
Email Address	John.barwick@hcpc-uk.org

Name and Telephone Number of Organisation's Personal Data Guardian/Caldicott Guardian	Claire Amor, Head of Governance (DPO) Claire.amor@hcpc-uk.org 020 840 9710

If you require the data to carry out work **on behalf of another organisation**, please complete the additional Table below. If not, please go straight to section (C).

Commissioning Organisation (if relevant)	
Name of Commissioning Organisation	
Contact Name	
Title	
Contact Number	
Email Address	

(C) Details of Identifiable Data Items required and rationale (NB. only minimum identifiable data should be requested for the required purpose)	
Please provide a list of data items that can identify an individual (e.g. Name, Address, Full Postcode, Date of Birth, HSC Number; Case-note Number; or other unique identifier that would link the data to identifiable details).	Please indicate the reasons for requiring each of these data items
1 __Full Name_____ 2__Full work address_____ 3 _Full home address_____ 4__Date of birth_____ 5__HCPC Registration number and profession 6__National Insurance number_____ 7__Nature of relevant disciplinary or health matter_____ 8__Telephone, mobile and email addresses if held	1Statutory notification of those potentially involved in fitness to practice matters from HCPC regulated professions _____ 2 a/a_____ 3__ a/a _____ 4 __ a/a _____ 5___ a/a _____ 6 ___ a/a _____ 7____ a/a _____ 8 __ a/a _____

9_____ 10_____ Continue on separate sheet if necessary	9_____ 10_____ Continue on separate sheet if necessary

Processing of information

Please complete all sections below to explain how information will be processed

- *complete all sections using language easily understood by lay reviewers*
- *continue on a separate sheet if necessary or attach any relevant documentation*

As a UK wide health and care regulator, HCPC requires notification of any registrant actions resulting in a disciplinary case. In turn HCPC informs employers of action against registrants taken by HCPC. Registrants suffering from some health conditions may also need to be notified to HCPC where their performance may be impacted. The overriding requirement is the protection of the public. Ongoing registration is required by the 15 professions, to use the protected titles within the UK.

Arts therapists, Biomedical scientists, Chiropodist / Podiatrists, Clinical scientists, Dietitians, Hearing aid dispensers, Occupational therapists, Operating department practitioners, Orthoptists, Paramedics, Physiotherapists, Practitioner psychologists, Prosthetists / orthotists, Radiographers, Speech and language therapists.

The purpose for which the data is required:
Information will initially be treated as confidential at HCPC's Fitness to Practise department. The data will be used to determine if a Fitness to Practise case is to be pursued against the data subject. The HCPC FTP processes will then be followed.
All PII will be transferred in encrypted form, using a complex password delivered by a different channel to the encrypted data file. This includes delivery of password via SMS.

How you propose to process the data once received: Please see the detailed descriptions and process maps in the links below.
The investigation process flowchart | (hcpc-uk.org)

HCPC data protection policy and privacy notice | (hcpc-uk.org)

Details of any record linking or matching to other data sources:

Once a registrant has been brought to our attention the original information alerting us to that potential case will become part of the bundle of evidence examined in that case. Therefore a link will be established initially on a temporary basis. The FTP department operate a separate database where cases are progressed. There is no ongoing logical (electronic link) between HCPC & RQIA systems. Data will only be exchanged on a case by case basis. If RQIA or other references are provided by RQIA within the terms of the MOU, these details may be retained for reference purposes.
Other relevant information:
Please list the System(s) from which data is to be extracted (if known) for Example PAS, SOSCARE, PARIS, NIECR, etc. Please also include sites or geographical locations (if known): iConnect

Frequency of transfers (*Please Tick*)	Once ☐ Other ☒ (Please specify) _As potential FTP cases are discovered or responded to by RQIA. or HCPC the other party will be alerted.

(D) Consent or other Lawful Basis for accessing personal data	
If you are requesting personal identifiable/special category data for a secondary purpose, there is an expectation that you will have explicit written consent from the service user(s) or another lawful basis for accessing their information. When relying on consent as the lawful basis, this means offering individuals genuine choice and control. This will require a very clear and specific statement of consent, which should be in writing and held on the service user's file. It should be clear to the individual what they are consenting to and who will have access to their information. It should be easy for individuals to withdraw consent and they should be made aware that they can do this at any time.	
Do you have the individuals' **informed**	Yes ☐ No ☒

consent for their data to be shared for the purpose specified in this DAA?	If yes, please provide a copy of the Consent Form with this application
If you are NOT obtaining informed consent, what other **lawful basis** are you relying on to obtain the data for this purpose? *(please discuss with your Data Protection Officer / IG department regarding relevant legislation and GDPR conditions –* *see Appendix 3 below re lawful basis under article 6 and article 9)*	As a UK wide Health & Care regulator, HCPC has a mandated requirement to investigate potential fitness to practice cases amongst its registrants. For more detail see section C above. **(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations). **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. Legal Obligation and Public Task _____ _Article 9 2 (c), (g), (i) Legislation | (hcpc-uk.org)
In the absence of consent or any other lawful basis, it will only be appropriate to share anonymous data or pseudonymous data (data pseudonymised at source). Please refer back to Section A.	

(E) Data Protection arrangements of the Organisation receiving the identifiable data – to provide assurance that the data shared is processed and stored securely by you, please answer the following questions:	
You must be registered with the Information Commissioner's Office (ICO) to process personal data. Please provide your **ICO registration number**	HCPC ICO registration**: Z6621691**
Do you have a confidentiality / privacy policy which complies with Data Protection legislation?	Yes ☒ No ☐
Are confidentiality clauses included within	Yes ☒ No ☐

contracts of all staff with access to the person identifiable information?	
Are all staff trained and aware of their responsibilities under Data Protection legislation and adhere to the Data Protection principles?	Yes ☒ No ☐
Do you have an ICT security policy?	Yes ☒ No ☐
Have you conducted a Data Protection Privacy Assessment (DPIA)? (please see App. 3 for further details on when a DPIA is necessary)	Yes x☐ No ☐ If yes please include a copy with this form.

(F) Measures / Controls in place by the receiving organisation to prevent the inappropriate disclosure of <u>Person Identifiable Information</u>	
How do you require the information to be securely transferred to your organisation?	Encryption (256-bit AES) of PII with the delivery of a password via a channel other than the delivery mechanism for the attachment.
Describe the physical security arrangements for the location where **person identifiable data** is to be: - processed; and - stored	Access controlled office space with logged entry by named individual. FTP information is loaded to a secure online case handling system on an ISO27001 certified platform Users may be working on site, or remotely via VPN or Windows Virtual Desktop offering inbuilt security. Data is generally stored electronically in G cloud environments, and replicated to secure alternate online data repositories
Provide details of access and/or firewall controls implemented on the system, and measures to encrypt which are in place.	Multiple levels of security have been implemented, (defence in depth) including firewalls, (however it is HCPC policy not to disclose details). HCPC has been certified to ISO27001 since 2015 and our Cyber Essentials Plus certification is under renewal..
Will this data be accessed or transferred by you to another organisation; or shared with another organisation?	Yes ☒ No ☐ (As part of the regulatory process)
If applicable, how will you secure information provided being transferred by you to another	RQIA data will form a minimal portion of data to be shared in case bundles. Any bulk PII

organisation?	transferred to / shared with other organisations will be encrypted and the password transferred by a channel other than that used to transport the encrypted file. The exact mechanism used depends on the capabilities of the organisation concerned. HCPC are required to share case information with the registrants legal advisors, and those assisting in the management of the case. Small amounts of data are shared by a secured portal on a case basis. Cases investigated by HCPC are audited by PSA (https://www.professionalstandards.org.uk)
Is a separate agreement in place to ensure the security of the data held by the 3rd party?	Yes ☒ No ☐ Data Sharing Agreements, Memoranda of Understanding or Data processing agreements are in place as appropriate.
If the data is to be stored or shared outside the UK please provide details (e.g. country):	HCPC only store information within the UK, or countries deemed adequate under GDPR. This excludes the USA.

(G) Data Retention – **Please indicate how long the receiving organisation will retain identifiable data**	
Please state the date by which you will be finished using the identifiable data. If this is not applicable you need to explain why?	hcpc-document-retention-policy.pdf (hcpc-uk.org)
If the data retention period for identifiable data is greater than two years, please indicate the reasons for this. (**The maximum data retention period is 2 years, after this time a review of this agreement is required**)	See table below for detailed description
Describe the method of data destruction you will employ when you have completed your work using person identifiable data	Electronic data will be purged from systems electronically, dependant on the retention schedule below.
HCPC Retention periods run from the date the case is closed or legal proceedings have ended and also applies to the physical evidence that has not been scanned onto the case management system.	

Description	period	Comment
Complaints that do not meet the HCPC Threshold Policy. (Includes closed MIS cases)	20 years	Information is retained in case further complaints are made.
Cases in respect of which an Investigating Committee Paneldetermines that there is no case to answer.	20 years	Information is retained in case further complaints aremade.
Cases in respect of which a case to answer decision was reached but which are discontinued by a Panel of the Conduct and Competence Committee or Health Committee before final hearing.	20 years	Information is retained in case further complaints aremade. A summary will be retained permanently.
Cases which a Panel of the Conduct and Competence Committee or Health Committee determines are not well founded.	Permanent	Information is retained in case further complaints aremade.
Cases that result in a sanctionimposed by the Conduct and Competence Committee or Health Committee.	Permanent	Information is retained in case further complaints are made.
Decisions of a Panel of the Conduct and Competence Committee or Health Committee when reviewing anorder under Article 30 of the Order.[2]	Permanent	Information is retained in case further complaints are made.

Description	period	Comment
Decisions of a Panel of the Conduct and Competence Committee or Health Committee in respect of applications for restoration under Article 33 of the Order.[3]	Permanent	It is to keep a record of thefact the registrant was restored (or restoration refused)to the register after being struck off.
Investigations in respect of offences under Article 39 and39A of the Order (where no prosecution follows).	20 years	Information is retained in case further complaints aremade.
Prosecutions in respect of offences under Article 39 and39A of the Order.[4]	Permanent	Information is retained in case further similar complaints are made.
Cases where a registrant has made a declaration in respectof their health/ character	20 years	Information retained for public protectionreasons.
Notifications about individuals not on the Register, who may apply for registration (including**FTP** information from overseasregulators).	20 years from last correspondence	Information retained for public protectionreasons.

[1] Art 37 of the Health and Social Work Profession Order 2001 (the Order) relate to appeals against decisions of the Education and Training Committee.

[2] Art. 30 of the Health and Social Work Profession Order 2001 (the Order) requires all conditions of practice orders and suspension orders to be reviewed before they expire.

When appropriate, please ensure that the Data Destruction Notification (Appendix 1) is completed within the specified retention period and returned to the appropriate contact person (see Appendix 4).

(H) Declaration: Organisation to which data will be shared

Please note that the completed Data Access Agreement will be immediately returned unless the receiving organisation has signed section H.

Data Protection Undertaking on Behalf of the Organisation Wishing to Access the Data

My organisation requires access to the data specified and will conform to Data Protection legislation; the Information Commissioner's Data Sharing Code of Practice; and the guidelines issued by the Department of Health in *"The Code of Practice on Protecting the Confidentiality of Service User Information (updated April 2019)".*

I confirm that:

- The information requested and any information extracted from it is for a specified, explicit and legitimate purpose
- It is adequate, relevant and limited to the stated purpose
- It will be processed fairly and lawfully and used only for the stated purpose
- It will be processed and stored in a manner that ensures appropriate security
- It will be held no longer than is necessary for the stated purpose
- It will be disposed of fully and in such a way that it is not possible to reconstitute it
- All measures will be taken to ensure identifiable data is not disclosed to third parties
- Where appropriate, the Health and Social Care organisation will be informed of the identifiable data being deleted / destroyed (see Appendix 1)
- In the case of pseudonymised data, the process of de-identifying data will be completed at source. The key to re-identification will be held only by the data controller and at no stage will the data we receive be attributed to an identified or identifiable natural person
- Any loss, theft or corruption of the shared data by my organisation will be immediately reported to the Personal Data Guardian / SIRO of the owning organisation and we will assist fully in any investigation. I understand that any serious breaches, data loss, theft or corruption will be reported to the ICO within 72 hours of the breach first being discovered.

As the Authorised Officer of the organisation to which data will be shared, I declare that I have read and understand my obligations and adhere to the conditions contained in this Data Access Agreement.

Signed: _____

(Personal Data Guardian / Caldicott Guardian / Authorised Officer)

Signed: **(IAO/SIRO)**
Claire Amor, Head of Governance

Date: **22/04/2022**_____

(I) Declaration – HSC Owner Organisation

DATA ACCESS AGREEMENT

I CONFIRM THAT:

The _____ (HSC owner organisation) consents to the disclosure of the data specified, to the organisation identified in Section B of this form. The disclosure of the data conforms to the guidelines issued by the Department of Health Code of Practice on Protecting Confidentiality of Service User Information (updated April 2019); and the Information Commissioner's Data Sharing Code of Practice.

Signed:  Mrs Jacqui Murphy (SIRO, RQIA) *(HSC Organisation internal use)*

(Information Governance and / or ICT Security)

Signed: **Dr Julie-Ann Walkden**
(PDG)_____

(Personal Data Guardian) OR (Senior Information Risk Owner SIRO)

25/04/2022

Date: _____

Please note that this organisation has the right to inspect the premises and processes of the requesting organisation to ensure that they meet the requirements set out in the agreement.

Appendix 1

Data Destruction Notification

(to be completed on all occasions when data is transferred external to HSC NI)

Authorised users of the person identifiable data have, under the terms and conditions of the Data Access Agreement, a requirement to destroy the data on or before the retention date stated in Section (G).

This form should be completed on destruction of the data, and returned to the relevant Trust contact (see Appendix 4):-

Data Destruction Notification	
Name of Organisation	
Name of Authorised Officer (please print)	
Position/Status	
Address	
Telephone Number	
Mobile Number (Optional)	
Fax Number	
Email Address	
Title of Agreement	
Date Declaration Signed	
Date Data Received	
Date Data Destroyed	

Signature	
Date	

Appendix 2 - Principles Governing Information Sharing[1]

Code of Practice Principles	GDPR Principles	Caldicott Principles[2]
The Code of Practice is principally concerned with identifiable service user information. The nature of the obligation to protect confidentiality can be expressed in terms of three core principles: • individuals have a fundamental right to the confidentiality and privacy of information related to their health and social care; • individuals have a right to control access to and disclosure of their own health and social care information by giving, withholding or withdrawing consent; • when considering whether to disclose confidential information, health and social care staff should have regard to whether the disclosure is necessary, proportionate and accompanied by any undue risks. Particular care is needed on the part of health and social care staff to ensure that the right to privacy of vulnerable people – specifically adults with incapacity and children – is respected and that the duty of confidentiality owed to them is fulfilled. https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentialityservice-user-information	**1.** processed lawfully, fairly and in a transparent manner **2.** Purpose limitation - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes **3.** Data minimisation - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **4.** Data Quality - accurate and, where necessary, kept up to date **5.** Storage Limitation - kept for no longer than is necessary. **6.** Integrity and Confidentiality - processed in a manner that ensures appropriate security of the personal data **7.** Overarching Accountability principle –take responsibility for what you do with personal data and how you comply with the other principles, having appropriate measures and records in place to be able to demonstrate your compliance. Principles relating to individuals' rights and overseas transfers of personal data are specifically addressed in separate GDPR articles.	**1.** Justify the purpose(s) for using confidential information. **2.** Only use it when absolutely necessary. **3.** Use the minimum that is required. **4.** Access should be on a strict need-to-know basis. **5.** Everyone must understand his or her responsibilities. **6.** Understand and comply with the law. **7.** The duty to share information can be as important as the duty to protect patient confidentiality

[1] These principles must be followed by health and social care organisations when considering use and disclosure of service user information.

[2] PDG Principles are adopted from the Caldicott Principles (revised September 2013) established in England and Wales.

Appendix 3 - Definitions

Personal Data
'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Consent
'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Processing
'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Pseudonymisation
'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Data Controller
'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Data Processor
'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Third party
'Third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (or DPIA) is part of the accountability obligations under the GDPR and is an integral part of the 'data protection by default and by design' approach. It is a process to help you identify and minimise the data protection risks of a project

A DPIA is mandatory when introducing a new system or process that is likely to include a high risk to the privacy of the individuals involved. An effective DPIA will document the data flows and help to identify and fix problems at an early stage, demonstrate compliance with data protection obligations, meet individuals' expectations of privacy and help avoid reputational damage which might otherwise occur. For further information please see:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Lawful Basis

You must have a valid lawful basis in order to process personal data. The conditions for processing personal data are included under article 6 of GDPR and for processing special category personal data under article 9.

There are six available lawful bases under Article 6 for processing personal data. No single basis is 'better' or more important than the others and the most appropriate basis to use will depend on your purpose and relationship with the individual. Most lawful bases require that processing is 'necessary' for a specific purpose. You must determine your lawful basis before you begin processing, and you should document it.

For full details of Article 6 lawful basis for processing personal data please refer to: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

In order to lawfully process 'special category data'*, you must identify both a lawful basis under Article 6 (in exactly the same way as for any other personal data); however you will also need to satisfy a specific condition under Article 9.

For full details of Article 9 lawful basis for processing personal data please refer to: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Special Category Data*

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Special category data is information about an individual's:

- race;

- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Appendix 4 - Contact details

Belfast Health and Social Care Trust

Gillian Acheson - Senior Data Protection Manager

Information Governance Dept | 1st Floor Admin Building | Knockbracken Health Care Park | Saintfield Road | Belfast BT8 8BH

Email: gillian.acheson@belfasttrust.hscni.net

Northern Health and Social Care Trust

Nicola Lyons - Information Governance Manager

Information Governance Department | Causeway House | Route Complex | 8E Coleraine Road | Ballymoney BT53 6BP |

E-mail: nicola.lyons@northerntrust.hscni.net

South Eastern Health and Social Care Trust

Lynda McAree - Head of Information Governance & Directorate Support

Information Governance Department | Lough House | Ards Community Hospital | Newtownards BT23 4AS

Email: Lynda.mcaree@setrust.hscni.net

Southern Health and Social Care Trust

Peter McManus - Information Governance Manager

Ferndale | Bannvale Site | 10 Moyallen Road | Gilford BT63 5JY

Email: Peter.McManus@southerntrust.hscni.net

Western Health and Social Care Trust

Jeremy Foster - Head of Records and Information Governance,

Trust Headquarters | MDEC Building | Altnagelvin Hospital site | Glenshane Road Londonderry BT47 6SB

Email: jeremy.foster@westerntrust.hscni.net

Public Health Agency
Karen Braithwaite - Senior Operations Manager (Delivery)

Public Health Agency | Tower Hill | ARMAGH | BT61 9DR

Email: Karen.Braithwaite@hscni.net

Health and Social Care Board

Ken Moore | Information Governance Manager

Corporate Services | Health and Social Care Board | Towerhill | Armagh | BT61 9DR | Northern Ireland

Email: Ken.Moore@hscni.net

Business Services Organisation

Alan McCracken - Data Protection Officer (DPO)

Business Services Organisation Headquarters | 2 Franklin Street | Belfast | BT2 8DQ

Email: Alan.McCracken@hscni.net