



**Isle of Man**  
Government

*Reillys Eilan Vannin*

Department of Health and Social Care

---

*Rheynn Slaynt as Kiarail y Theay*

# **CQC Inspection of Relevant Service Providers**

## **Data Protection Impact Assessment**

Project Name	<b>CQC Inspection of Relevant Service Providers</b>
Controller	<b>Department of Health and Social Care</b>
Data Protection Officer	Rebecca Evans
Business Owner/Senior Responsible Owner/Project Manager	Julie King – Director Quality, Safety and Engagement
DPIA Completed By	Paul Edge
Job title	Head of Corporate Compliance/SIRO
DPIA Reference	<b>DHSC/2022/0002</b>

## Document Management

### Revision History

Version	Date	Summary of Changes
1	4 Feb 2022	Removal of typo, para 2
2	8 Feb 2022	Inclusion of inspection pilot[s] date of commencement 21 <sup>st</sup> February 2022
3	16 Feb 2022	Removal of ref to schedule 9 HASC Act
4	11 Jul 2022	Inclusion of Relevant Service Provider Employee checks for transparency

### Document Control:

The controlled copy of this document is maintained in the DHSC corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity

## Contents:

<b>Section 1</b> .....	4
Part 1 - Data Protection Impact Assessment.....	4
Screening Questionnaire.....	4
Part 2 - Data Protection Impact Assessment.....	7
Additional Questions.....	7
<b>Section 2</b> .....	9
Data Protection Impact Assessment.....	9
1. Care Quality Commission.....	9
2. Department of Health and Social Care.....	9
3. Definitions.....	10
4. Schedule of Inspections.....	12
5. The Legal Basis for Processing Data.....	13
6. Common Law Duty of Confidentiality.....	16
7. The Human Rights Act 2011.....	19
8. Deceased Patients.....	21
9. Transparency.....	21
10. CQC – Necessity Test.....	22
11. Assessment.....	25
12. Risk to Individuals.....	36
13. Identify and Assess Risk.....	38
14. Measures to Mitigate (Treat) Risk.....	40
15. Post-treatment Assessment.....	43
16. Stakeholder Engagement Matrix.....	44
17. Further Actions.....	45
18. Signatories.....	45
19. Summary of High Residual Risks.....	45
<b>Staff Guidance</b>	
Appendix 1: Principles relating to processing of personal data (Article 5).....	48
Appendix 2: Guidance for completing legal grounds for processing personal data (Article 6).....	49
Appendix 3: Guidance for completing legal grounds for processing special categories of data (Article 9).....	51
Appendix 4: The Eight Caldicott Principles.....	54
Appendix 5: Guidance for Completing a Risk Register.....	56
Appendix 6: What is a Data Protection Impact Assessment?.....	58
Appendix 7: Glossary.....	64

## Section 1

### Part 1 - Data Protection Impact Assessment

#### Screening Questionnaire

Section 1 is a 'Screening Questionnaire' to decide if a full Data Protection Impact Assessment (DPIA) is necessary.

Determining whether a data protection impact assessment (DPIA) is required should occur as early as practicable in the lifecycle of a project and, in all cases, prior to the commencement of processing.

If it is determined that a DPIA is required then the resources required to do so, the individuals who will need to be involved, and the timeframe for the DPIA, including referral to the Commissioner when required, should also be identified.

The risks to individuals may not be apparent at an early stage of a project; the requirement for a DPIA may, therefore, need to be reconsidered, reviewed or repeated as the project moves forward.

A DPIA is not required to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. A DPIA is only mandatory where processing is **"likely to result in a high risk to the rights and freedoms of individuals"**.

In cases where it is not clear whether a DPIA is required one is to be carried out regardless. It is a useful tool.

To understand if you will be processing personal data and special categories of personal data under the Applied GDPR, complete the data items table below.

Data Items	YES	NO
<b>Personal Data</b>		
Name	✓	
Address	✓	
Postcode	✓	
DOB	✓	
Age	✓	
Sex	✓	
Marital Status	✓	
Gender	✓	
Living Habits	✓	
Professional Training / Awards	✓	
Income / Financial / Tax Situation		✗
Email Address	✓	
Physical Description	✓	
General Identifier e.g. NHS No	✓	
Home Phone Number	✓	
Online Identifier e.g. IP Address / Event		✗
Website Cookies		✗
Mobile Phone Number / Device Number	✓	
Device IMEI No		✗
Location Data (Travel / GPS / GSM Data)		✗



Device MAC Address (Wireless Network Interface)		X
<b>Special Categories of Personal Data</b>		
Physical / Mental Health or Condition	✓	
Sexual Life / Orientation	✓	
Family / Lifestyle / Social Circumstance	✓	
Offences Committed / Alleged to have Committed	✓	
Criminal Proceedings / Outcomes / Sentence		X
Education / Professional Training	✓	
Employment / Career History	✓	
Financial Affairs		X
Religion or Other Beliefs		X
Trade Union membership		X
Racial / Ethnic Origin	✓	
Biometric Data		X
Genetic Data	✓	
<b>Additional Information (If Applicable)</b>		
<p>The Care Quality Commission ('CQC') is the independent regulator of health and social care in England.</p> <p>The CQC's programme will begin with an <b>initial validation phase</b>, to establish the end-to-end process and baseline for inspections. In <b>phase two</b> an approach to inspections will be developed, and service providers will be asked to share their views. The <b>third phase</b> will see the proposed operating model tested and rolled out, with inspections undertaken by CQC in three key areas: hospitals, primary care services (covering GPs, dental care, minor injuries and out of hours) and adult social care.</p>		

**Note:**

1. If the answer to any of the data items is “**Yes**” then personal data is being processed and the following nine questions need to be answered.
2. If all the answers are “**No**” then you do not need to answer the nine questions and the DPIA screening questionnaire is complete [submit to the DHSC DPO for QA]

If personal data is being processed, use the questionnaire [Page 7] to determine whether a full DPIA is necessary.

Should the answer to any screening question be “**Yes**” then a full DPIA is to be carried out.

**Note:**

1. Advice can be sought from the Data Protection Officer and/or the Senior Information Risk Owner on completion of the DPIA.
2. Additional advice is provided in [Appendix 6](#) - What is a Data Protection Impact Assessment? Of this document, also;

- The Information Commissioner has produced guidance on <sup>1</sup>Data Protection Impact Assessments available [here](#)

**At a glance:**

How do I identify which lawful basis applies?

Checklist:

- What kind of information is being processed?
- What is your purpose?
- Can you reasonably achieve it in a different way?
- Do you have choice over whether or not to process the data?
- Is the processing compatible with our lawful vires?

The Department is committed in ensuring that the fundamental rights of data subject's is always first and foremost when processing personal data.

*Lawful bases vs individuals' rights*

	Right of Access	Right to Rectification	Right to Erasure	Right to Restrict Processing	Right to Portability	Right to Object
Consent	✓	✓	✓	✓	✓	✗
Contract Necessity	✓	✓	✓	✓	✓	✗
Legal Obligation	✓	✓	✗	✓	✗	✗
Vital Interest	✓	✓	✓	✓	✗	✗
Public Interest	✓	✓	✗	✓	✗	✓
Legitimate Interests	✓	✓	✓	✓	✗	✓

But right to withdraw consent

<sup>1</sup> Information Commissioner – Data Protection Impact Assessments <https://www.inforights.im/media/1558/data-protection-impact-assessmentsv2.pdf>



## Part 2 - Data Protection Impact Assessment

### Additional Questions

Serial	Section	Yes	N/A	Unsure (Explain)
1	Does the proposal involve any evaluation or scoring including profiling & predicting using information about a person?		✓	
2	Does the proposal involve any automated decision making which has a legal or similar legal effect e.g. whether to employ an individual, grant them a loan or offer medical insurance?		✓	
3	Does the proposal involve any systematic monitoring: processing used to observe, monitor or control individuals, including data collected through networks e.g. employees' activities, including the monitoring of the employees' work station, internet activity; monitoring of wellness, fitness and health data via wearable devices; closed circuit television; connected devices e.g. smart meters, smart cars, home automation; includes internet tracking and profiling for behavioural advertisement?		✓	
4	Does the proposal involve any sensitive information or information of a highly personal nature e.g. health?	✓		
5	Does the proposal involve data processed on a large scale? Large scale is not defined but should consider: A) The number of data subjects, either as a specific number or as a proportion of the relevant population. B) The volume of data and/or the range of different data items processed. C) The duration, or performance of the data processing activity. D) The geographical extent of the processing activity. Processing of patient data in the regular course of business by a hospital would be classed as "large scale" while processing of patient data by an individual physician would not.		✓	
6	Does the proposal involve any matching or combining of datasets? i.e. matching two or more data processing operations		✓	

	performed for different purposes in a way that would exceed the reasonable expectations of an individual.			
7	Does the proposal involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, patients and cases where an imbalance in the relationship between the position of the individual and the controller can be identified.	✓		
8	Does the proposal involve any innovative use or applying new technological or organisational solutions e.g. combining use of finger print and face recognition for improved physical access control?		✓	
9	Does the proposal involve any processing which in itself 'prevents data subjects from exercising a right or using a service or contract' e.g. determining eligibility based on an individual's circumstances?		✓	

**Author assessment:**

Due to the processing of limited and necessary sensitive data and confirmation by completion of the DPIA screening assessment, a full DPIA is required, noting in particular that CQC inspection is a new novel processing activity on island, and taking into account the nature, scope, context and purposes of the processing, could be likely to result in a high risk to the rights and freedoms of natural persons.

Prior consultation with the Information Commissioner under Article 35(1) and Article 36(1) of the Applied GDPR is required.



## Section 2

### Data Protection Impact Assessment

#### 1. Care Quality Commission

The [Care Quality Commission](#) ('CQC') in England has powers of inspection and entry and to require documents and information under the <sup>2</sup>Health and Social Care Act 2008 (an Act of Parliament) Sections 76 to 79 govern the CQC's use and disclosure of confidential personal information. Section 80 requires the CQC to consult on and publish a code of practice on how it obtains, handles, uses and discloses confidential personal information ('CPI')

The <sup>3</sup>Code established the practices that CQC follows to **obtain, handle, use and disclose confidential personal information**. Access to confidential personal information plays an essential role in CQC's inspections and the wider regulation of health and social care services in England.

Importantly, the CQC have produced a Protecting your privacy when using your information [leaflet](#) which states

##### Protecting your privacy

*We don't look at everybody's information as part of an inspection. In most cases we will only look at a small sample of records, or where we have specific concerns about a person's care.*

*We only make a copy of information if we really need to, for example if we find evidence of poor care and we need to take action against a service. (Author: CQC regulatory action does not extend to the Isle of Man)*

*We make sure that we keep personal information securely and we don't keep it for longer than necessary.*

*If you don't want CQC inspectors to look at information about you, please tell your care provider so they can make a note about your preference. We will not usually look at the records of someone who does not want us to.*

#### 2. Department of Health and Social Care

The Department of Health and Social Care ('DHSC') redesigned on 1 April 2021 as a direct result of Sir Jonathan Michael's [Independent Review of the Isle of Manx Health and Care System](#). This Review continues to be a catalyst for change and improved service provision. The redesigned DHSC ensures the separation between the setting of policy and strategy and the delivery of services by [Manx Care](#).

---

<sup>2</sup> Health and Social Care Act 2008 <https://www.legislation.gov.uk/ukpga/2008/14/contents>

<sup>3</sup> CQC Code of practice on confidential personal information September 2016 (reviewed and amended in May 2018 to reflect updates to legislation in 2018) <https://www.cqc.org.uk/files/code-practice-confidential-personal-information>

Improving services isn't enough in itself. Behind it we need a structure of good governance, clarity on what we will deliver by when, how we will deliver these goals and assurance that the right oversight and reporting is in place. The relationship between the Department and Manx Care is designed to achieve that. The Department has set out its strategy and annual priorities within the [Mandate to Manx Care](#). The Department will hold Manx Care accountable for the delivery of services, the outcomes, and any directed efficiencies.

The Department has commissioned the CQC under Section 7, Part 3 – Inspections, of the [Manx Care Act 2021](#) to inspect service[s] provided by a relevant service provider under the Mandate.

Improving services and ensuring the safety of patients and service users are the key aims of a new approach to the external inspection of health and social care services Island-wide.

The CQC has been asked by the Department of Health and Social Care to assist in developing a system of independent inspections of Manx Care services, providing assurance to Government and the public that services are safe and of high quality.

A key recommendation of [Sir Jonathan Michel's independent review of the Island's health and care system](#) was: *that regular external inspections should be carried out on services provided directly by Manx Care, or by others on its behalf, reporting back to the Manx Care Board and the DHSC.*

Service assurance across health and social care is the responsibility of the Quality, Safety and Engagement team within DHSC, which retains responsibility for the [Registration and Inspections Team](#) (R&I). The R&I team will continue to inspect a wide range of care services and settings, including those provided by external contractors.

Alongside existing inspections, the new arrangement will provide external scrutiny and validation to ensure services meet **high quality and safety standards** and that any problems are identified and resolved. It will also highlight areas and teams which are delivering excellent services.

The same level of scrutiny and feedback will be applied to services in the Isle of Man as to those in England, and the CQC team will also provide professional advice and assistance to Manx Care and DHSC. However, while CQC will inspect, monitor and provide shadow ratings for health and care services in the Island, it will not have the power to enforce change or act as a regulator. This is the responsibility of DHSC to monitor and ensure that Manx Care is taking appropriate steps to address any issues raised.

### 3. Definitions

The following definitions of terms used within this document are taken from Article 4 of the Applied GDPR:

**'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;

**‘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.

**‘Restriction of processing’** means the marking of stored personal data with the aim of limiting their processing in the future

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

**‘Recipient’** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

**‘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;

**‘Profiling’** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

**‘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.

**‘Filing system’** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

**‘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

**‘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.

**‘Processor’** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.



**‘Personal data breach’** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

**‘Data concerning health’** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

**‘Genetic data’** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

**‘Supervisory authority’** means an independent public authority which is established by a Member State pursuant to Article 51 of the Applied GDPR

## 4. Schedule of Inspections

Inspections of the following Mandated Services are expected to commence during the second Service Year (the original Mandate stated ‘first’ service year, however due to COVID and contractual arrangements, inspections will begin with pilot inspections commencing 21<sup>st</sup> February 2022 and then endure throughout the service delivery year 2022)

The following list details those Mandated Services that are expected to be inspected by the CQC (subject to contractual agreement and therefore the Department retains the right to amend the schedule list of inspections as applicable)

- Adult Social Services
- Older People
- Learning Disability Services
- Social Work and Support Services
- Hospital, Mental Health and Communities
- Community Services
- Community Adult Nursing
- Community Children and Families
- Community Allied Health Professionals Services
- Children and Families Services
- Adult Social Care
- Mental Health Services
- Screening Services
- Sexual Health Services
- Unscheduled Care
- Scheduled Care
- Women’s & Children’s Integrated Services
- Diagnostics & Therapies
- Patient Safety & Quality
- Primary Care
- General Practice
- Dental Services

- Pharmacy services
- Ophthalmic Services

**Author assessment:**

Mandated Services as ‘controllers’ will need to ensure access to personal data, to provide such information which is required by the inspectors (‘CQC’) for the proper performance of the inspection is lawful, proportionate, adequate and relevant. Access to patient/staff administration systems with the correct access control, permission and audit facility is the responsibility of the controller.

The Mandate is available [here](#) for further information

## 5. The Legal Basis for Processing Data



The legal basis for CQC to undertake inspections of relevant service providers will be:

**Applied GDPR Art. 6 (1)(e)** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller to meet the statutory obligations under **Section 1 of NHS Act 2001**, to provide a comprehensive health service and **Schedule 1, Part 3, Section 7 of the Manx Care Act 2021** Inspections arranged by the Department

**Applied GDPR Art. 9 (2)(g)** processing is necessary for reasons of substantial public interest, on the basis of Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

**Applied GDPR Art. 9 (2)(h)** processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or

social care systems and services on the basis of Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

The Table of Functions below, for full completeness, demonstrates the lawful basis of the CQC undertaking inspections of relevant service providers under the Mandate.

Legislation	Relevant to:
<p><a href="#">Isle of Man National Health Service Act 2001</a></p> <p>NHS Act 2001 Pt 1, Section 1</p> <p><i>Part 1 – Administration</i>  <i>Section 1 Duty of Department</i>  <i>(1) The Department of Health and Social Care (“the Department”) shall —</i>  <i>(a) continue to promote in the Island a comprehensive health service designed to secure improvement in —</i>  <i>(i) the physical and mental health of the people of the Island, and</i>  <i>(ii) the prevention, diagnosis and treatment of illness, and</i>  <i>(b) for that purpose provide or secure in the Island or elsewhere the effective provision of services in accordance with the following provisions of this Act.</i></p>	<p>Department of Health and Social Care</p>
<p><a href="#">Manx Care Act 2021</a></p> <p>Manx Care Act 2021 Part 2, Section 4</p> <p><i>Part 2 – Duties and responsibilities of the Department [pg 6]</i></p> <p><i>s4 Promotion of comprehensive health and social care service</i>  <i>(1) Without prejudice to the following provisions of this Act, the Department must continue to promote in the Island a comprehensive health and social care service to secure improvement in —</i>  <i>(a) the physical and mental health of people in the Island;</i>  <i>(b) the prevention, diagnosis and treatment of physical and mental illness;</i>  <i>(c) the provision of social care services for people in the Island.</i></p>	<p>Department of Health and Social Care</p>
<p><a href="#">Manx Care Act 2021</a></p> <p>Manx Care Act 2021 Part 3, Section 13</p> <p><i>Part 3 — Manx Care and the Mandate [pg 10]</i></p>	<p>Manx Care</p>



<p>s13 <i>Manx Care and its general functions</i></p> <p>(1) <i>Such of the functions of the Department referred to in section 4 which are the subject of the mandate, must be discharged by Manx Care on behalf of the Department in accordance with the mandate, applicable regulations and any directions given to Manx Care.</i></p> <p>(2) <i>In discharging those functions of the Department referred to in subsection (1) Manx Care must promote in the Island a comprehensive health and social care service, and in doing so has—</i></p> <p>(a) <i>the functions of providing and arranging for the provision of services for the purposes of the health and social care service in the Island in accordance with this Act; and</i></p> <p>(b) <i>the duties referred to in Part 4.</i></p>	
<p><a href="#">Manx Care Act 2021</a></p> <p><i>Manx Care Act 2021 Part 3, Section 14</i></p> <p>(1) <i>Before the start of each financial year, the Department must publish and lay before Tynwald a document to be known as “the mandate”.</i></p> <p>(2) <i>The mandate must include the matters specified in Schedule 2 (which has effect for that purpose) and may include other matters.</i></p> <p>(3) <i>The Department may by regulations amend Schedule 2. Tynwald procedure — approval required.</i></p> <p>(4) <i>Manx Care must seek to achieve the objectives specified in the mandate, and comply with any requirements specified in it.</i></p> <p>(5) <i>Before specifying any objectives or requirements in the mandate, the Department must consult and have due regard to the views of—</i></p> <p>(a) <i>Manx Care;</i></p> <p>(b) <i>in respect of public health, such persons whom it considers are suitably qualified to advise on such matters by virtue of their training or experience; and</i></p> <p>(c) <i>such other persons as the Department considers appropriate.</i></p> <p>(6) <i>The Department must keep Manx Care’s performance in achieving any objectives or requirements specified in the mandate, applicable regulations and directions under review.</i></p>	<p>Department of Health and Social Care &amp; Manx Care</p>
<p><a href="#">Manx Care Act 2021</a></p> <p><i>Manx Care Act 2021 Schedule 1, Part 3, Section 7</i></p> <p><i>Part 3 Inspections, Section 7 Inspections arranged by the Department</i></p> <p><i>Section 7</i></p>	<p>Department of Health and Social Care, Care Quality Commission &amp; Manx Care (Relevant Service Provider)</p>

<p><i>(1) This paragraph applies to a service provided by a relevant service provider under the mandate.</i></p> <p><i>(2) The Department must in each year draw up —</i></p> <p><i>(a) a schedule specifying the service or services (or a specific matter connected to such a service) in respect of which an inspection will be undertaken in that year (a “scheduled inspection”); and</i></p> <p><i>(b) a list of services which the Department is minded to arrange an inspection of in each of the next two successive years.</i></p> <p>.....</p> <p><i>(8) An inspection must be conducted by one or more appropriate independent persons or bodies (“inspectors”) appointed by the Department.</i></p> <p><i>(10) It is the duty of a relevant service provider to —</i></p> <p><i>(a) assist inspectors undertaking an inspection; and</i></p> <p><i>(b) provide such information which is required by the inspectors for the proper performance of the inspection.</i></p>	
--	--

For the avoidance of doubt, Section 7(11) defines relevant service provider as:

**(11) “Relevant service provider” means—**

- (a) Manx Care where it provides the services in question under the mandate;*
- (b) a person with whom Manx Care has entered into an agreement under section 17 of this Act and who is based, and provides those services in the Island;*
- (c) both Manx Care and such a person or persons where the services in question are provided by them jointly.*

.....

**Manx Care and/or Relevant Service Provider Employees**

CQC will also inspect employee records in regards to Mandatory Training, Disclosure Barring Service (DBS) checks, Professional Certificates, evidence of Employment History, References obtained (Yes or No), Indemnity Insurance expiry dates if applicable, photographic Identification, professional registration reference no & date (where applicable), Start Date, Last Appraisal/ Performance review date, Qualification Type and certificate date.

**6. Common Law Duty of Confidentiality**

The common law duty of confidentiality (‘CLDC’) is not codified; it is based on previous judgements in court. Whilst various interpretations of the common law may be possible it is

widely accepted that, where information which identifies individual patients/service users is provided and held in confidence, disclosure may only be justified in one of three ways

- the patient/service user has given consent for their information to be used;
- the balance of public and private interest favours public interest disclosure; or
- a statutory basis exists which permits or requires disclosure

Evidencing service user consent or a statutory basis under the common law is straightforward. Consent is obtained or there is a statutory basis under which the sharing can happen.

Satisfying the public interest under the common law is considerably more complex. It is about assessing the benefits and risks of sharing the information and basing a decision on that analysis.

However, Confidentiality can be overridden by legislation or where there is sufficient public interest justification. The public interest test involves making a balanced judgment taking account of the strong public interest in maintaining public trust in the provision of confidential services with the public interest in favour of disclosure and the private interests of any individuals involved. The nature and extent of the disclosure will be a key factor in arriving at a balanced and proportionate judgment.

Recent case law indicates that the common law duty of confidentiality would generally continue to apply after the death of an individual. It also needs to be borne in mind that clinical records often contain third party information relating to living persons and therefore that a duty of confidence is likely also to be owed to these individuals.

But the common law cannot be considered in isolation. Even if a disclosure of confidential information is permitted under the common law, the disclosure must still satisfy the requirements of data protection law.



**Author assessment:**

CLDC is set aside for **proportionate, relevant and adequate** access to CPI by CQC to undertake inspections of relevant service providers under the following statutory basis:

Manx Care Act 2021 Schedule 1, Part 3, Section 7

(1) This paragraph applies to a service provided by a relevant service provider under the mandate.

(2) The Department must in each year draw up —

(a) a schedule specifying the service or services (or a specific matter connected to such a service) in respect of which an inspection will be undertaken in that year (a “scheduled inspection”); and

(b) a list of services which the Department is minded to arrange an inspection of in each of the next two successive years.

.....

(8) An inspection must be conducted by one or more appropriate independent persons or bodies (“inspectors”) appointed by the Department.

(10) It is the duty of a relevant service provider to —

(a) assist inspectors undertaking an inspection; and

(b) provide such information which is required by the inspectors for the proper performance of the inspection.

The Table below summarises the commonly used bases and sets out when a patient opt-out applies. Options include the use of the legal gateways set out in the Public Health (Notifiable Diseases) Order 2011, as an example, which allow confidential patient information to be used without patient consent:

Legal basis in Common Law	Opt-out applies	Comments
Common Law Consent (Implied)	No – out of scope for the patient data opt-out	<p>For common law purposes the sharing of information for direct or individual care purposes is on the basis of implied consent. This is out of scope for a patient data opt-out - which only applies to purposes beyond individual care.</p> <p><b>Note:</b> This is included in this table for completeness and to emphasise that implied consent can only be used when the surrounding circumstances mean that a patient knows, or would reasonably expect, that their data will be shared. In other words there should be ‘no surprises’ for the individual about who has had access to information about them where implied consent is relied upon.</p> <p>An individual will still be able to ask their doctor or other healthcare professional</p>

		not to share a particular piece of information with others involved in providing their care and should be asked for their explicit consent before access to their whole record is given.
Common Law Consent (Explicit)	No	In this case an individual has given their consent for a specific use of their data, for example consenting to participate in a research study. This would fall within the general exemption from a patient data opt-out.  This rule applies even if the consent was given before the patient had set a data opt-out
Mandatory legal requirement	No	Where there is a legal requirement for the data disclosure that specifically sets aside the common law duty of confidentiality then a patient data opt-out will not apply.
Mandatory legal requirement - example	No	Data disclosure under <a href="#">Section 2 of the Public Health (Notifiable Diseases) Order 2011</a>

Therefore, when determining if patient opt-outs will apply requires the following to be clearly established:

- Purpose - it is for a purpose beyond individual care, and
- The basis for the disclosure in common law

However, please refer to [Paragraph 10](#) CQC Necessity Test for assurance.

## 7. The Human Rights Act 2011

The Human Rights Act 2001 ('HRA') incorporates the fundamental rights and freedoms in the European Convention on Human Rights into Manx domestic law.

The Act makes it unlawful for a public authority to behave in a way which contravenes those rights. This means that all public authorities must ensure that everything they do is compatible with [Convention](#) rights unless an Act of Tynwald makes that impossible.

People are entitled to expect that public authorities respect their Convention rights.

The Human Rights Act means that:

- Convention rights and responsibilities form a common set of binding values for public authorities

- Public authorities must have human rights principles in mind when they make decisions about people's rights
- Human rights must be part of all policy making
- All legislation must be interpreted and given effect as far as possible, compatibly with the Convention rights.
- It is unlawful for a public authority to act incompatibly with the Convention rights and allows for a case to be brought in the Isle of Man Courts against the authority if it does so

The Department is subject to the HRA and due consideration must always be given when making a decision about people's rights.

A person's right to have their privacy respected is protected by Article 8 of the ECHR. This right is not absolute, and may be interfered with where the law permits and where it is *'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The Right to Respect for Private and Family Life contains four rights.

These are:

- The right to respect for private life
- The right to respect for family life
- The right to respect for one's home
- The right to respect for correspondence

Article 8 is not an absolute right, in that the HRA makes provision for interference with the right if it is lawful and proportionate to do so.

### Interference with an Article 8 right

Article 8 rights are qualified rights; this means that in certain circumstances they can be interfered with by the state.

However, this interference must be **lawful**, for a **legitimate social aim** and **necessary** to achieve that aim.

Furthermore, the interference must not be disproportionate to the objective to be achieved.

Legitimate social aims are:

- National security
- Protection of public safety
- Protection of health or morals
- Prevention of crime or disorder
- Protection of the economic well-being of the country
- Protection of the rights and freedoms of others

The Department will have to weigh up the public interest necessity of breaching an Article 8 right against the rights of the individual.

### **Author assessment:**

The Human Rights Act (Article 8) gives individuals a right to respect for their private and family life. However, this does not make it unlawful for organisations to process personal data where there is otherwise a lawful basis to do so.

A public authority abiding by the Applied GDPR and the CLDC is likely to meet the Human Rights Act obligations. This is because the Applied GDPR's overarching aim is the protection of the rights and freedoms of individuals where it concerns the handling of their personal data. However, it will be important to ensure that any information sharing is necessary for the specified purpose AND is proportionate.

The CQC is appointed by the Department under Schedule 1, Part 3, Section 7(8) of the Manx Care Act 2021.

It is the duty of a relevant service provider under Schedule 1, Part 3, Section 7(10)(b) of the Manx Care Act 2021 to provide such information which is required by the inspectors for the proper performance of the inspection.

The overarching inspection function is to protect and promote the health, safety and welfare of people who use health and social care services, consistent with the legitimate social aim for the protection of health or morals.

## **8. Deceased Patients**

A patient data opt-out continues to be maintained and applied for an individual after they have died. Health and adult social care organisations are expected to continue to apply opt-outs for deceased patients.

## **9. Transparency**

Data protection legislation requires that the collection and processing of personal data is **fair, lawful and transparent**.

This means there must always be a valid lawful basis for the collection and processing of data as defined under data protection legislation, and the requirements of the CLDC must also be met.

As well as having a duty to be fair and a lawful basis for collection and processing of data, all controllers must also be transparent.

Transparency is an important element of data protection. All controllers must make sure that individuals know how their data is used and for what purposes it is shared.

There should be '**no surprises**' for an individual in terms of how their data is used



Articles 13 and 14 of the Applied GDPR specify what individuals have the right to be informed about.

This right forms the key transparency requirement of the Applied GDPR and requires controllers to provide individuals with all the information necessary to understand what will happen to their personal data, how it will be protected, how long it will be kept, where it may be transferred to, and to know what rights they have in relation to that data. This is often known as 'privacy information'.

Controllers are required to provide privacy information:

- in a concise, transparent, intelligible and easily accessible form
- in clear, plain language adapted as necessary to meet the target audience needs, especially where children, or other vulnerable groups, are concerned
- in conjunction, if needed or desirable, with standardised icons to give an easily visible, intelligible and clearly legible overview of the intended processing.

Controllers can use a 'privacy notice' or 'fair processing' information to inform individuals, or use other methods. By law, the information provided should be **concise, easy to understand and easily accessible**

#### **Author assessment:**

The Department will produce and make available communications informing citizens and health and social care providers of the proposed inspections, specifications and purpose to be undertaken by the CQC.

It is the responsibility of all relevant service providers 'controllers' to provide individuals with all the information necessary to understand what will happen to their personal data, how it will be protected, how long it will be kept, where it may be transferred to, and to know what rights they have in relation to that data.

The Information Commissioner has produced an authoritative and extremely useful suite of information regarding Transparency – Information about processing [here](#)

## 10. CQC – Necessity Test

The necessity test is the foundation that CQC uses to make all decisions about whether they should obtain, use or disclose confidential personal information. This applies whether or not consent is required.

Using this test helps to make sure that CQC is acting fairly and lawfully by establishing need, assessing competing interests and considering any potential for damage, loss or distress. It enables CQC to recognise and balance the implications of their actions against the potential harm that may be caused if they do not act.

CQC staff use this test frequently, and it will help others to understand how CQC are likely to use their information.

Section 80 of the Health and Social Care Act 2008 (an Act of Parliament) requires the CQC to prepare and publish a code in respect of the practice it proposes to follow in relation to confidential personal information

### **Section 80 Code of practice on confidential personal information**

(1) *The Commission must prepare and publish a code in respect of the practice it proposes to follow in relation to confidential personal information.*

(2) *The code must in particular make provision—*

*(a) about the obtaining by the Commission of information which, once obtained, will be confidential personal information, and*

*(b) about the handling, use and disclosure by the Commission of confidential personal information*

The 'necessity test' is detailed within the [code](#) along with established practices that the CQC follow to obtain, handle, use and disclose confidential personal information.

#### **Author assessment:**

The inspection regime will fully respect individuals rights to privacy and is aligned to the following Caldicott Principles (see [Appendix 4](#))

#### **Principle 2: Use confidential information only when it is necessary**

*Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.*

#### **Principle 4: Access to confidential information should be on a strict need-to-know basis**

*Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes*

#### **Principle 5: Everyone with access to confidential information should be aware of their responsibilities**

*Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.*

#### **Principle 6: Comply with the law**

*Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.*

**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. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required*

## 11. Assessment

Data Protection Principle: Lawfulness, Fairness and Transparency [\[Article 5\(1\)\(a\)\]](#)

Question	Response	Comments
<p>What is the legal basis for processing the personal data?</p>	<p>Identified</p>	<p>Section 1 of the National Health Service Act 2001 and Schedule 1, Part 3, Section 7 of the Manx Care Act 2021</p> <p>Article 6(1)(e) and Articles 9(2)(h) and 9(2)(g)</p> <p>Inspections must comply with the law by minimising the use of identifiable data. To meet the data protection principles when using personal data, the amount of data should be adequate, relevant, and not excessive for the purpose.</p> <p>For individual care purposes, service providers can receive and share special category personal data or confidential personal information (CPI) by ensuring that they meet the lawful processing conditions as controllers.</p> <p>Article 30 ROPA will need to be updated.</p> <p>Noting: Is the power being exercised for a lawful purpose?</p> <ul style="list-style-type: none"> <li>a) If a public authority acts outside its power for a purpose that the power was not created to achieve, the action will be 'ultra vires' – <b>Legal basis identified</b></li> <li>b) The purpose of the power may be expressly set out in legislation, or it may be implied from its objectives. – <b>Purpose identified</b></li> </ul>



		c) A public authority has a power to undertake tasks ‘conducive to’ or ‘reasonably incidental to’ a defined purpose. – <b>Power identified</b>
Is the processing of an individual's personal data likely to interfere with the ‘right to privacy’ under <a href="#">Article 8 of the Human Rights Act</a>	No	<p>The Human Rights Act (article 8) gives individuals a right to respect for their private and family life. However, this does not make it unlawful for organisations to process personal data where there is otherwise a lawful basis to do so. A public authority abiding by the Applied GDPR and the CLDC is likely to meet the Human Rights Act obligations.</p> <p>This is because the Applied GDPR's overarching aim is the protection of the rights and freedoms of individuals where it concerns the handling of their personal data.</p> <p>The overarching inspection function is to protect and promote the health, safety and welfare of people who use health and social care services, consistent with the legitimate social aim for the protection of health or morals.</p>
Is there a Privacy Notice explaining to individuals how their personal data will be used? (If so, please attach a copy)	No – To be developed if approved.	<p>Communications and engagement professionals will be utilised within the transparency process. It is important to ensure that the production of materials, language and channels used are appropriate. To ensure consistency throughout the project, it is important that the same messages and language are used.</p> <p>Care will be taken if conveying information to children, as more specific obligations will apply. The ICO has guidance regarding <a href="#">Children's data</a> and the processing of their data.</p> <p>The law gives discretion to controllers to consider where this information is displayed and which different layers of communication to adopt.</p> <p>It is however clear that information regarding the processing of personal data must be:</p> <ul style="list-style-type: none"> <li>• easily accessible (paper or electronic if requested or directed to the website)</li> <li>• concise, transparent and intelligible</li> <li>• written in clear, plain language</li> <li>• free of charge</li> </ul>

		<p><b>Note:</b> The duty of transparency is also one of the ways we can build trust and gain the respect of the public in the use of their data. The aim of transparency is to ensure there are ‘no surprises’ for the patient. This is now enshrined as the eighth <a href="#">Caldicott Principle</a> - <b>Inform patients and service users about how their confidential information is used.</b></p> <p>Patients and service users have the right to know certain information about the processing of their personal data by health and care organisations.</p> <p>These include:</p> <ul style="list-style-type: none"> <li>• the purpose for processing</li> <li>• what information is being processed</li> <li>• who is processing their information</li> <li>• if they have the right to rectification or erasure of their data</li> <li>• the right to complain to the ICO</li> <li>• where information about them is collected from (if not themselves)</li> </ul> <p>This list is not exhaustive, and this information will need to be included within the all relevant controllers transparency materials created for patients and/or service users’ ref CQC inspections.</p>
<p>If you are relying on consent to process personal data, how will consent be obtained and recorded?</p>	<p>No – however, consent is not the basis for processing</p>	<p>All patients have the right to opt out of sharing or providing additional information, CQC will follow their own necessity test etc.</p>
<p>Do you receive personal data about individuals from third parties?</p>	<p>Yes, though proportionate and relevant</p>	<p>CQC reviews confidential personal information, including information from medical and care records, because at times it is a necessary way of helping us to understand the quality of people’s care and to ensure that we achieve our purpose of making sure people receive safe, effective, compassionate, high-quality care, and encouraging services to improve.</p>

<p>Can data subjects exercise their rights under the Applied GDPR?</p>	<p>Yes – each controller will need to ensure data subjects are informed via their own Transparency requirements under the Applied GDPR and update RoPA.</p> <p>DHSC will need to update Transparency information and RoPA</p>	<p>Data subject rights are:</p> <ul style="list-style-type: none"> <li>• ✓ Be informed</li> <li>• ✓ Get access to it</li> <li>• ✓ Rectify or change it</li> <li>• ✗ Erase or remove it</li> <li>• ✓ Restrict or stop processing it</li> <li>• ✗ Move, copy or transfer it</li> <li>• ✓ Object to it being processed or used</li> <li>• ✓ Know if a decision was made by a computer rather than a person</li> </ul> <p>Transparency information to be updated</p> <p>Public engagement to be progressed</p> <p>Article 30 RoPA's to be updated</p>
--	---	---

Data Protection Principle: Purpose Limitation [\[Article 5\(1\)\(b\)\]](#)

Question	Response	Comments
Can your project or initiative be achieved by using pseudonymised or anonymised data only?	No	CQC reviews confidential personal information, including information from medical and care records, because at times it is a necessary way of helping us to understand the quality of people's care and to ensure that we achieve our purpose of making sure people receive safe, effective, compassionate, high-quality care, and encouraging services to improve.
Does your project or initiative involve the use of existing personal data for new purposes?	Yes	CQC inspections are a new and novel process.
Are potential new purposes for the personal data likely to be identified?	No	None
Who are the recipients of the personal data?	CQC	As per inspection criteria



Data Protection Principle: Adequate, Relevant and Limited [\[Article 5\(1\)\(c\)\]](#)

Question	Response	Comments
Can your project or initiative be achieved by using pseudonymised or anonymised data only?	No	Partially, access to confidential personal information plays an essential role in CQC's inspections and the wider regulation of health and social care services.  CQC reviews confidential personal information, including information from medical and care records, because at times it is a necessary way of helping us to understand the quality of people's care and to ensure that we achieve our purpose of making sure people receive safe, effective, compassionate, high-quality care, and encouraging services to improve.
Does your project or initiative involve the use of existing personal data for new purposes?	Yes	CQC inspection
Are potential new purposes for the personal data likely to be identified as the scope of your project or initiative expands?	No	None

Data Protection Principle: Accuracy [\[Article 5\(1\)\(d\)\]](#)

Question	Response	Comments
How is personal data checked for accuracy?	Verification	<p>Individuals have a right to have inaccurate personal data rectified or completed if it is incomplete. These requests can be made verbally or in writing and organisations have one calendar month to respond.</p> <p>In certain circumstances, organisations can refuse a request for rectification. (Note, this right is closely linked to controllers obligations under the accuracy principle of the Applied GDPR [Article (5) (1) (d)].</p> <p>The following relevant statements from the NHS Constitution (2013, 2015) and how this right may be applied should also be noted:</p> <p><i>“You have the right to have any factual inaccuracies corrected. Ask your health professional about amending your records if you believe they contain a factual error.”</i></p> <p><i>“There is no obligation to amend professional opinion, however, sometimes it is difficult to distinguish between fact and opinion. Where you and the health professional cannot agree on whether the information in question is accurate, you can ask that a statement is included to set out that the accuracy of the information is disputed by you”</i></p> <p>(page 56) <a href="#">The Handbook to the NHS Constitution 2013</a>.</p>
What action would be taken to correct inaccurate personal data?	Controller	<p>As above – patient to inform controller</p> <p>Controller responsibility:</p> <ul style="list-style-type: none"> <li>carefully consider any challenges to the accuracy of personal data by a data subject;</li> </ul>

		<ul style="list-style-type: none"> <li>• respond to the individual without undue delay and within one month to communicate the action, or inaction, taken;</li> <li>• communicate the rectification to each recipient it has been disclosed to (Article 19);</li> <li>• if the individual has requested to be informed about those recipients, communicate those details to the individual (Article 19).</li> </ul> <p>Refusing a request</p> <p>Controllers may refuse to comply with all or part of the request for rectification but must be able to justify its decision.</p> <p>Requests may be refused in cases where:</p> <ul style="list-style-type: none"> <li>• the request is manifestly unfounded or excessive, in particular if it is repetitive (Article 12(5));</li> <li>• a restriction on the right can be justified in the particular circumstances (Article 23)</li> </ul>
How frequently is the personal data updated or what would trigger the information being updated?	Ad Hoc	Dependent on interaction between data subject and controller
Is the quality of the information good enough for the proposed purposes?	Yes	Though dependent on the coded activity and accuracy of data.
Are the sources of the personal data recorded?	Yes	<p>Yes – sourced direct from the patient/service user record.</p> <p>Access to patient administration systems - User, Time/Date and reason for access recorded.</p>

Data Protection Principle: Storage Limitation [\[Article 5\(1\)\(e\)\]](#)

Question	Response	Comments
What are the retention periods for the personal data and how often are these reviewed?	10 years	However that is the lifecycle retention of the Inspection report, personal data will not form part of the inspection report
What is the justification for holding the personal data for this length of time?	Legal obligation	NHS Records Management Code of Practice 2021 <a href="#">Read the code of practice online</a> (HTML) <a href="#">Download the code of practice</a> (PDF, 1MB)
How will the retention schedule be managed and enforced?	DHSC	SOP, Policy and Procedures
How will personal data be fully anonymised, archived or destroyed after it is no longer needed?	DHSC	SOP, Policy and Procedures



Data Protection Principle: Appropriate technical and organisational measures [\[Article 5\(1\)\(f\)\]](#)

Question	Response	Comments
<p>What procedures are in place to ensure that all staff with access to personal data have adequate Information Governance (IG)/Data Protection training?</p>	<p>Policies and procedures</p> <p>RBAC to be clearly defined and managed (on boarding / off boarding)</p> <p>Robust audit process</p>	<p>Adopting the principles of data protection by design and data protection by default is an important concept for any project or new model of care. It is important that when considering new ways of working, the impact to privacy and confidentiality are factored in at the design stage – Controllers will need to ensure appropriate access is granted via own policy/procedures</p> <p>That way IG is integrated into the policies, processes and systems from the beginning. It will assist in enabling data sharing for the benefit of individuals and the system, whilst minimising the risk to privacy.</p> <p>Training is critical on use and viewing combined with a robust audit process to ensure an effective RBAC access control model which:</p> <ul style="list-style-type: none"> <li>(1) allows proportionate access to appropriate and relevant data held within an individual's health and care record if deemed necessary by the CQC</li> <li>(2) creates robust audit on each access which can be investigated and challenged, if deemed inappropriate</li> </ul>
<p>How is access removed when someone leaves the project, or no longer needs access to the data?</p>	<p>Strict on boarding / off boarding policy and procedure to be implemented by each viewing organisation</p>	<p>Removal of RBAC code - controller responsibility.</p> <p>Robust audit policy and procedures to be implemented - controller responsibility.</p> <p>Staff training</p>
<p>Please describe the technical and security controls associated</p>		<p>Patient or service users have the right to challenge that access.</p>

<p>with your project or initiative</p>		<p>Any unauthorised access is to be treated as a ‘personal data breach’. The Applied GDPR introduces a duty on all organisations to investigate security incidents to establish whether a personal data breach has occurred. Therefore, a robust breach detection, investigation and internal reporting procedures will need to be in place.</p> <p>[REDACTED]</p> <p>Policy and Procedures</p> <p>Compliance to HRA, DPA, CLDC and professional codes of conduct.</p> <p>[REDACTED]</p> <p>Adopting ‘Data Protection by Design’ (embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage) and ‘Data Protection by Default’ (service settings must be automatically data protection friendly)</p> <p>While long recommended as good practice, both of these principles are enshrined in law under the GDPR (Article 25).</p>
--	--	---

## 12. Risk to Individuals

Many requirements of the Applied GDPR including security, appropriate measures, records of processing activities, data protection impact assessments etc., require a consideration of the **"risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing"**

An objective assessment should be undertaken to establish whether the processing operations involve a risk, or in some cases, a high risk, **to the individual**, and the likelihood and severity of that risk.

**Whilst reputational damage is important, the objective assessment must consider risks to the data subject first and foremost.**

The following are broad examples of the **risks** to the individual that the processing of data may lead to:

- Physical damage
- Material damage
- Moral damage

### 1. Effect on the individual:

- Discrimination
- Identity theft or fraud,
- Financial loss,
- Damage to the reputation,
- Loss of confidentiality of data protected by professional secrecy,
- Unauthorized reversal of pseudonymisation, or
- Any other significant economic or social disadvantage

### 2. Where data subjects might be **deprived of their rights and freedoms or from exercising control over their personal data;**

### 3. Where special categories of personal data are processed:

- Racial or ethnic origin,
- Political opinions,
- Religion or philosophical beliefs,
- Trade-union membership,
- The processing of genetic data or
- Data concerning health or sex life or
- Criminal convictions and offences or
- Related security measures;

### 4. Profiling - where personal aspects are evaluated, in particular analysing or prediction of aspects concerning:

- Performance at work,
- Economic situation,

- Health,
  - Personal preferences or interests,
  - Reliability or behaviour,
  - Location or movements,
  - In order to create or use personal profiles;
5. Where personal data of **vulnerable individuals**, in particular of **children**, are processed;
6. Where processing involves a large amount of personal data and affects a large number of data subjects

See Recitals 74-77

Other recitals refer to risk in relation to the following areas:

**Recital 28** – pseudonymisation

**Recital 38** - children's data

**Recital 51** - special categories of data

**Recital 71** - profiling

**Recital 83** - encryption

**Recital 84 & 90/91** - Data protection impact assessments

Examples of **high risk processing** (in connection with data protection impact assessments) can be found in Article 35(3) of the Applied GDPR and Appendix 6



### 13. Identify and Assess Risk

Consider the potential impact of your processing and the potential harm or damage that it might cause to individuals whether physical, emotional, moral, material or non-material e.g. inability to exercise rights; discrimination; loss of confidentiality; re-identification of pseudonymised data, etc.

Describe source of the risk and nature of potential impact on individuals		Likelihood of harm (Remote; reasonable possibility or more likely than not)	Severity of impact (Minimal impact; some impact; or serious harm)	Overall risk rating (Low; Medium; or High)		
R01	Legal vires to proceed challenged or not accepted by ICO – unable to proceed, limited inspection regime – <b>ultra vires</b>	Reasonable Possibility	Serious Harm	HIGH		
				4	5	20
R02	Public mistrust regarding use of and sharing of patient information resulting in a lack of confidence within the health and care system - <b>confidentiality</b>	More Likely than Not	Serious Harm	HIGH		
				5	4	20
R03	Patient Administration Systems unable to issue appropriate access control – <b>availability, integrity</b>	Remote	Minimal Impact	LOW		
				3	2	6
R04	[REDACTED]	Reasonable Possibility	Some Impact	MEDIUM		
				4	4	16
R05	[REDACTED]	Reasonable Possibility	Serious Harm	HIGH		
				4	4	16
R06	Relevant service providers not providing to CQC relevant information to fulfil their function – <b>availability, quality, completeness, contract</b>	Reasonable Possibility	Serious Harm	HIGH		
				4	4	16



Describe source of the risk and nature of potential impact on individuals		Likelihood of harm (Remote; reasonable possibility or more likely than not)	Severity of impact (Minimal impact; some impact; or serious harm)	Overall risk rating (Low; Medium; or High)		
R07	[REDACTED]	Reasonable Possibility	Serious Harm	HIGH		
				4	4	16
R08	Poor data quality, un-coded episodes of care resulting in lack of information presented to CQC - <b>inaccurate data, integrity, availability</b>	Reasonable Possibility	Serious Harm	HIGH		
				5	5	25
R09	Function creep – personal data used for non-defined purposes, or requested access by non-health or care organisations - <b>confidentiality</b>	Reasonable Possibility	Serious Harm	HIGH		
				4	5	20
R10	Data subjects unable to exercise their lawful rights, not provided full information on the proposed processing – <b>compliance, transparency,</b>	Reasonable Possibility	Serious Harm	HIGH		
				4	5	20

## 14. Measures to Mitigate (Treat) Risk

Against each risk you have identified, record the options/controls you have put in place to mitigate the risk and what impact this has had on the risk. Make an assessment as to the residual risk.

Risk	Options to mitigate (Treat) the risk	Effect on risk [Tolerate/Terminate/ Treat/Transfer]	Residual risk [Low/Medium/High]	Owner (organisation)
<b>R01</b>	1. Native risk – prior consultation with ICO required under the Applied GDPR	Treat	High	DHSC
<b>R02</b>	1. Public information program to be launched prior to processing 2. Dedicated FAQ to be drafted and provided to the public/stakeholders 3. Consultation with ICO 4. Consultation with external stakeholders	Treat	Medium	DHSC
<b>R03</b>	1. Controllers (Relevant Service Provider) to ensure appropriate and necessary access controls are issued	Treat	Low	Relevant Service Provider
<b>R04</b>	1. Controllers (Relevant Service Provider) to follow their own policy and procedures once access is no longer required	Treat	Low	Relevant Service Provider

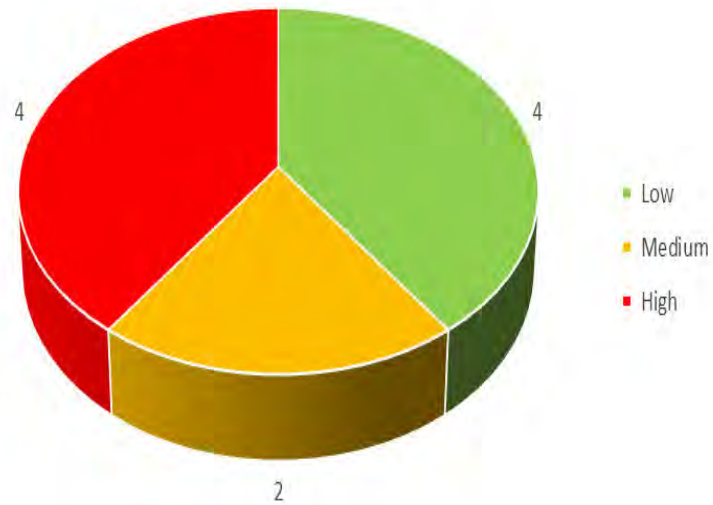
Risk	Options to mitigate (Treat) the risk	Effect on risk [Tolerate/Terminate/ Treat/Transfer]	Residual risk [Low/Medium/High]	Owner (organisation)
R05	1. Controllers (Relevant Service Provider) to liaise with processor if applicable, follow local policy and procedures	Treat	Low	Relevant Service Provider
R06	1. Phased roll-out agreed 2. DHSC engagement with citizens/relevant service providers 3. Scope of inspections defined 4. RBAC control to be clearly defined 5. Lawful vires established	Treat	High	DHSC/Relevant Service Provider
R07	[REDACTED]	Tolerate	High	[REDACTED]
R08	1. Controllers (Relevant Service Provider) Native Risk – Inspection outcomes to determine	Tolerate	High	Relevant Service Providers



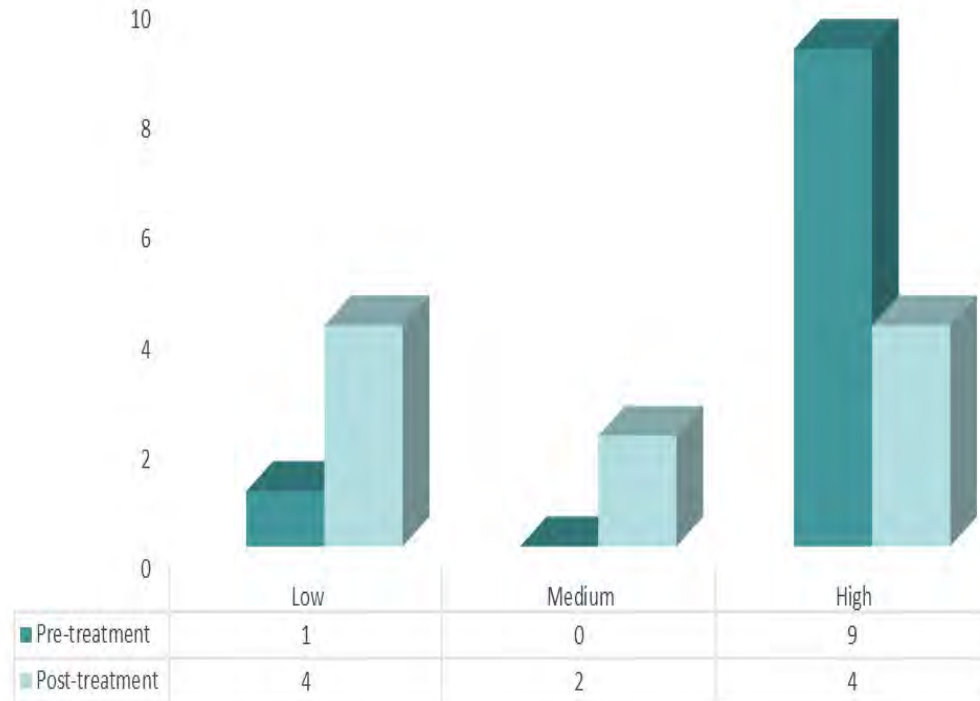
Risk	Options to mitigate (Treat) the risk	Effect on risk [Tolerate/Terminate/ Treat/Transfer]	Residual risk [Low/Medium/High]	Owner (organisation)
<b>R09</b>	<ol style="list-style-type: none"> <li>1. Inspection scope defined</li> <li>2. Control of CPI defined for lawful purpose only</li> </ol>	Treat	Low	DHSC
<b>R10</b>	<ol style="list-style-type: none"> <li>1. Public engagement and communication</li> <li>2. Stakeholder engagement</li> <li>3. Transparency information updated</li> <li>4. DPIA undertaken and to be published on DHSC website</li> </ol>	Treat	Medium	DHSC/All Controllers

## 15. Post-treatment Assessment

Number of post-treatment risks



Number of risks by risk level pre and post treatment





## 16. Stakeholder Engagement Matrix

Consultation with the following internal/external stakeholders undertaken during the completion of the DPIA

Organisation/Individual	Comments	Accepted [Yes / No]	Integrated back into project plan and Owner
DHSC			
Manx Care			
Health and Care Transformation			
Patient Representatives'			

## 17. Further Actions


The completed DPIA should be submitted to the DHSC DPO:

**Email:** [DPO-DHSC@gov.im](mailto:DPO-DHSC@gov.im)

## 18. Signatories

The DPIA accurately reflects the processing and the residual risks have been mitigated as reasonably practicable and/or resolved by the Senior Responsible Officer/Project Manager.


**Senior Responsible Officer/Project Manager - Signature and Date**

 03 February 2022
---

---

**FOR OFFICE OF THE DHSC DPO AND SIRO USE ONLY**

## 19. Summary of High Residual Risks

Risk No.	High Residual Risk Summary
R01	Treat - Lawful vires challenged, may result in the Department implementing Policy which is ultra vires. Processing breaching HRA, CLDC and DPA
R06	Treat – Engagement, collaboration – Native Risk
R07	
R08	Tolerate – Native risk – Inspection outcomes to determine

## Summary of DPO advice

I am satisfied that the legal vires have been established and proposed processing identifies the rights of data subjects first and foremost. A DPIA is a living document so must be updated to reflect any changes to processing and/or scope and be resubmitted to the DHSC Office of the DPO and SIRO for assurance.

Rebecca Evans 03 February 2022

## ICO consultation outcome

In considering the DPIA I particularly noted the quality of the objective risk assessment that was undertaken.

In my view the DHSC does have the statutory power to require such inspections to be undertaken and as indicated in the DPIA the CQC also has a vires to do so. I would, however, recommend that the DHSC seek the advice of the Attorney General's Chambers if it has not done so already.

The proposal is intended to analyse, measure and improve the quality of health care provided to the Manx public.

I am satisfied that the DPIA has objectively, systematically and comprehensively assessed the proposed processing, considered the risks that may arise and appropriate mitigations. The intended processing should therefore comply with the data protection legislation.

In my opinion the proposal accords with the principle of putting the patient first.

Information Commissioner 04 February 2022

## Next Steps:

- DPO to inform stakeholders of ICO consultation outcome
- Identified risk mitigation and/or remedial actions to be assigned ownership and integrated back into the project plan
- If processing is approved, Privacy Notices' to be updated
- Article 30 Register of Processing Activity to be updated
- Training to be provided to staff
- Public information program to be initiated and launched
- Phased implementation of access as per roll out

## Sources of Authority:

1. Isle of Man Information Commissioner - <https://www.inforights.im/> [accessed 1 February 2022]
2. European Court Of Human Rights – Guide on Article 8 of the European Convention on Human Rights, *Right to respect for private and family life, home and correspondence* – Updated 31<sup>st</sup> August 2021 [ [www.echr.coe.int/documents/guide\\_art\\_8\\_eng.pdf](http://www.echr.coe.int/documents/guide_art_8_eng.pdf) ] [accessed 1 February 2022]
3. NHS Digital – National Data Opt-Out <https://digital.nhs.uk/services/national-data-opt-out> Last edited: 4 June 2021 [accessed 1 February 2022]
4. European Commission - *Guidelines on Data Protection Impact Assessment (DPIA)* (wp248rev.01) date 13 October 2017 <https://ec.europa.eu/newsroom/article29/items/611236> [accessed 1 February 2022]
5. Gov.UK - *Review of data security, consent and opt-outs* – National Data Guardian – Published 6 July 2016 <https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs> [accessed 2 February 2022]
6. NHS Digital – *Cyber and data security*, <https://digital.nhs.uk/cyber> [accessed 2 February 2022]
7. Care Quality Commission – *Code of practice on confidential personal information* <https://www.cqc.org.uk/get-involved/consultations/code-practice-confidential-personal-information> [accessed 2 February 2022]

## References:

1. EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20 October 2020 (Version 2.0).
2. EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20 October 2020 (Version 2.0), p. 18. Along the same lines, CJEU, 1 October 2015, Bara, C-201/14 (available [here](#)).
3. *Herbst* in Kühling, Buchner, DS-GVO BDSG, Article 5 GDPR, margin number 66 (Beck 2021, 3rd ed.) (accessed 9 December 21)
4. WP29, Guidelines on Transparency under Regulation 2016/679, 11 April 2018 (available [here](#))
5. NHS Digital, DCB Compliance with National Data Opt-outs, release number AMD 91/2018, 18 March 2019 (available [here](#)) (accessed 14 December 2021)
6. *Georgieva, Kuner*, in Kuner et al., The EU General Data Protection Regulation (GDPR), Article 9 GDPR, p. 379 (Oxford University Press 2020).
7. EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, [p. 20](#).
8. The CJEU shares the same conclusions: “*in the light of the purpose of the directive, the expression 'data concerning health' used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual*”. See, CJEU, 6 November 2003, Bodil Lindqvist, C-101/01, margin number 50 (available [here](#))
9. WP29, Opinion 03/2013 on purpose limitation, 2 April 2013, p. 16 (Available [here](#))
10. WP29, Guidelines on Transparency under Regulation 2016/679, 11 April 2018, [p. 7](#)
11. European Court of Human Rights. *Amann v. Switzerland* [GC], no. [27798/95](#).
12. European Court of Human Rights. *Rotaru v. Romaina* [GC], no [28341/95](#)

## Appendix 1: Principles relating to processing of personal data (Article 5)

### <sup>4</sup>Article 5

#### Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (*'lawfulness, fairness and transparency'*);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (*'purpose limitation'*);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (*'data minimisation'*);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (*'accuracy'*);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (*'storage limitation'*);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (*'integrity and confidentiality'*);

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (*'accountability'*)

#### Relevant Recitals

**Recital 39:** Principles of Data Processing Expand

**Recital 74:** Controller Responsibility and Liability

---

<sup>4</sup> Data Protection (Application of GDPR) Order 2018 [SD No. 2018/0143] Article 5 Principles relating to processing of personal data [Page 93]

[https://www.legislation.gov.uk/cms/images/LEGISLATION/SUBORDINATE/2018/2018-0143/DataProtectionApplicationofGDPROrder2018\\_2.pdf](https://www.legislation.gov.uk/cms/images/LEGISLATION/SUBORDINATE/2018/2018-0143/DataProtectionApplicationofGDPROrder2018_2.pdf)



## Appendix 2: Guidance for completing legal grounds for processing personal data (Article 6)

### <sup>5</sup>Article 6

#### Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

#### Relevant Recitals:

- Recital 39:** Principles of Data Processing
- Recital 40:** Lawfulness of Data Processing
- Recital 41:** Legal Basis or a Legislative Measure
- Recital 42:** Proof and Requirements for Consent
- Recital 43:** Freely Given Consent
- Recital 44:** Processing in the Context of a Contract
- Recital 45:** Legal Basis in Union or Member State Law
- Recital 46:** Vital Interest of a Natural Person
- Recital 47:** Overriding Legitimate Interests
- Recital 48:** Data Transfers Within a Group of Undertakings
- Recital 49:** Network and Information Security as a Legitimate Interest
- Recital 50:** Compatible Purpose for Further Processing
- Recital 171:** Repeal of Directive 95/46/EC and Transition Phase

---

<sup>5</sup> Data Protection (Application of GDPR) Order 2018 [SD No. 2018/0143] Article 6 Lawfulness of processing [Page 96]

[https://www.legislation.gov.uk/cms/images/LEGISLATION/SUBORDINATE/2018/2018-0143/DataProtectionApplicationofGDPROrder2018\\_2.pdf](https://www.legislation.gov.uk/cms/images/LEGISLATION/SUBORDINATE/2018/2018-0143/DataProtectionApplicationofGDPROrder2018_2.pdf)

## Guidance Note:

Article 6 contains specific requirements that must be met to make the processing of personal data 'lawful'. These are known variously as the 'legal basis', 'condition', or 'ground', for processing

In order to process 'special category data', a controller must demonstrate that one of the exceptions to the prohibition on processing special category data applies (See Appendix 3)

In respect of 'personal data', processing shall be lawful **only if and to the extent that** at least one of the following applies:

- the data subject has given [consent](#) to the processing of his or her personal data for one or more specific purposes;
- processing is **necessary** for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is **necessary** for compliance with a legal obligation laid down by Manx law or Union law as applied to the Island to which the controller is subject;
- processing is **necessary** in order to protect the vital interests of the data subject or of another natural person;
- processing is **necessary** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller which is laid down by Manx law or Union law as applied to the Island;
- processing is **necessary** for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (NOT applicable to processing of personal data carried out by a public authority in the performance of their tasks).

With the exception of consent, each condition for processing is qualified by the phrase “**processing is necessary**”. This phrase has been considered by the Court of Justice of the European Union in *Huber v Germany* and is generally taken to mean that the processing is “proportionate to the legitimate aim being pursued” (for example, see [Stone v SE Coast Strategic Health Authority \[2006\] EWHC 1668 \(Admin\)](#))

## Appendix 3: Guidance for completing legal grounds for processing special categories of data (Article 9)

### <sup>6</sup>Article 9

#### **Processing of special categories of personal data**

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
  - (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
  - (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
  - (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
  - (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
  - (e) processing relates to personal data which are manifestly made public by the data subject;
  - (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
  - (g) processing is necessary for reasons of substantial public interest, on the basis of Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
  - (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

---

<sup>6</sup> Data Protection (Application of GDPR) Order 2018 [SD No. 2018/0143] Article 9 Processing of special categories of personal data [Page 96]

[https://www.legislation.gov.im/cms/images/LEGISLATION/SUBORDINATE/2018/2018-0143/DataProtectionApplicationofGDPROrder2018\\_2.pdf](https://www.legislation.gov.im/cms/images/LEGISLATION/SUBORDINATE/2018/2018-0143/DataProtectionApplicationofGDPROrder2018_2.pdf)

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union law (as applied to the Island by or under the authority of an Act of Tynwald) or Manx law or rules established by national competent bodies.
4. Member States (including, for these purposes, the Island) may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

## **Guidance Note:**

### Special categories

The processing of "special categories" of personal data is prohibited unless an exception set out in Article 9(2) applies.

The 'special categories' are defined in Article 9(1) of the Applied GDPR. Recitals 51-54 of the Applied GDPR provide additional narrative on special category data

Special categories include personal data revealing

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- health or sex life
- unique identity of a person by processing biometric or genetic data

Before the Department may start processing special category data **we must** be able to demonstrate that one of the exceptions to the prohibition on processing set out in Article 9(2) applies and, with the exception of "[explicit consent](#)", it is necessary to process that special category data.

In summary, the exceptions are:

- explicit consent (unless law prohibits the processing and that prohibition cannot be overridden by the person)



- legal obligation on the controller in respect of employment, social security etc.
- protection of the vital interests of the data subject or another person where the data subject is legally or physically incapable of giving consent
- legitimate activities of a non-profit making organisation with a political, philosophical or trade-union aim
- the personal data is manifestly made public by the data subject
- necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- substantial public interest (based on Manx law or Union law applied to the Island) which is proportionate to the aim pursued, respects the essence of the right to data protection and provides specific measures to protect the fundamental rights and freedoms of the data subject
- necessary for the purposes of preventative or occupational medicine, assessment of working capacity, medical diagnosis, provision of health or social care or treatment or the management of health and social care systems and services (on the basis of Manx law or Union law applied to Island)
- public health (on the basis of Manx law or Union law applied to Island)
- archiving in the public interest, research and statistics (on the basis of Manx law or Union law applied to Island)

You must complete a [Data Protection Impact Assessment](#) or 'DPIA' if the intended processing is likely to result in a high risk to the rights and freedoms of natural persons and if you intend to process special category data on a large scale – Further advice can be obtained from the DPO and/or SIRO

#### Note:

Personal data relating to criminal convictions and offences is not classed as "special category data" but is separately defined in Article 10 of the Applied GDPR. Any processing of such personal data, can only be carried out in accordance with Article 10, i.e. under the control of official authority or when authorised by Manx law or Union law applied to Island.

All Controllers must be aware of the types of personal data they process and which of the relevant grounds for processing, or exception to the prohibition on processing, is being met.

## Appendix 4: The Eight Caldicott Principles

Good information sharing is essential for providing safe and effective care. There are also important uses of information for purposes other than individual care, which contribute to the overall delivery of health and social care or serve wider public interests.

These principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

The principles are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses. In some instances, the principles should also be applied to the processing of staff information.

They are primarily intended to guide organisations and their staff, but it should be remembered that patients, service users and/or their representatives should be included as active partners in the use of confidential information. Where a novel and/or difficult judgment or decision is required, it is advisable to involve a Caldicott Guardian.

### **Principle 1: Justify the purpose(s) for using confidential information**

*Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.*

### **Principle 2: Use confidential information only when it is necessary**

*Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.*

### **Principle 3: Use the minimum necessary confidential information**

*Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.*

### **Principle 4: Access to confidential information should be on a strict need-to-know basis**

*Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.*

### **Principle 5: Everyone with access to confidential information should be aware of their responsibilities**

*Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.*

## **Principle 6: Comply with the law**

*Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.*

## **Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality**

*Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.*

## **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. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.*

### **Additional information:**

Guidance, issued under the National Data Guardian's statutory powers, about the appointment, role and responsibilities of Caldicott Guardians, available [here](#)

### **GOV.UK**

<https://www.gov.uk/government/publications/national-data-guardian-guidance-on-the-appointment-of-caldicott-guardians-their-role-and-responsibilities>

National Data Guardian guidance on the appointment of Caldicott Guardians, their role and responsibilities and new free online learning (24 December 2021)

### **Caldicott Guardian online learning launched**

The Role of the Caldicott Guardian online learning

An elearning programme, The Role of the Caldicott Guardian, is for Caldicott Guardians and those with an interest in finding out more about they do to keep people's data safe, and ensure that wise decisions are made about its use.

The programme offers three, audience specific modules:

A module for all staff: Caldicott Guardians: sharing information and protecting confidentiality in health and care

The aim of this session is to raise awareness and inform a broad range of staff from across health and social care of the importance of Caldicott Guardians and confidentiality in their setting, organisation, or sector. The learning would benefit staff working in the NHS, adult social care, local authorities and private sector partners.

Elearning for healthcare: <https://www.ukcqc.uk/elearning-resources>

## Appendix 5: Guidance for Completing a Risk Register

1. What is the actual risk? Make sure the risk is clear and concise and articulated with appropriate use of language, suitable for the public domain.
2. Be careful and sensitive about the wording of the risk as risk registers are subject to the Freedom of Information (FOI) requests.
3. Don't reference blame to other organisations in the risk register (the register may be made available in the public domain).
4. Does the risk belong to a business area within your organisation or another body?

It is common to use a RAG matrix rating system for assessing risk.

RAG stands for **Red**, **Amber**, and **Green**

To achieve a RAG rating, each risk first needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

IMPACT: How major could the consequences be if the risk event happened?

	INSIGNIFICANT 1	MINOR 2	SIGNIFICANT 3	MAJOR 4	SEVERE 5
ALMOST CERTAIN 5	MEDIUM 5	MEDIUM 10	HIGH 15	HIGH 20	HIGH 25
LIKELY 4	LOW 4	MEDIUM 8	HIGH 12	HIGH 16	HIGH 20
MODERATE 3	LOW 3	MEDIUM 6	MEDIUM 9	HIGH 12	HIGH 15
UNLIKELY 2	LOW 2	LOW 4	MEDIUM 6	MEDIUM 8	MEDIUM 10
RARE 1	LOW 1	LOW 2	LOW 3	LOW 4	MEDIUM 5

LIKELIHOOD: What are the chances of the risk event happening?

### The privacy risk assessment methodology

The goal of any privacy information risk assessment methodology is to make sure everybody conducting the assessment or interpreting its findings are on the same page.

You must have a methodology – e.g. a set of rules defining how to conduct the risk assessment – to make sure the risks are evaluated consistently, enabling you to adequately compare your priorities.

Methodologies also outline specific terms for the Department:

- Baseline security criteria: the minimum set of defences to fend off risks;
- Risk scale: a universal way of quantifying risk;
- Risk appetite: the level of risk the Department is willing to accept; and
- Scenario- or asset-based risk management: the strategies to reduce the damage caused by certain incidents or that can be caused to certain parts of the organisation

When assessing and determining whether information is to be processed or to assess whether adequate processes have been put in place, the risk matrix is a fundamental instrument that is generally compiled by the Department

For assistance identifying associated risks contact the DPO and/or the SIRO



## Appendix 6: What is a Data Protection Impact Assessment?

*"Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community."*

[Z v Finland \(1997\) 25 EHRR 371, 405](#), at [95]

When is a Data Protection Impact Assessment (DPIA) required?

A DPIA is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is required at least in the following cases:

- a systematic and extensive evaluation of the personal aspects of an individual, including profiling;
- processing of sensitive data on a large scale;
- systematic monitoring of public areas on a large scale

The DPIA should be conducted before the processing and should be considered as a living tool, not merely as a one-off exercise. Where there are residual risks that can't be mitigated by the measures put in place, the DPIA must be consulted prior to the start of the processing.

A Data Protection Impact Assessment (DPIA) is a method by which a controller can **objectively, systematically and comprehensively** assess the proposed processing of personal data and identify, and minimise, the risks to an individual when developing a new, or updating an existing, system.

The fundamental aim is to weigh the need for, and the potential benefit of, the processing against the impact on individuals. An effective DPIA can provide compliance, financial and reputational benefits, which help demonstrate accountability and assist a controller build trust and confidence with individuals.

A DPIA should commence early in the life of a project, whether at the point of design or before purchasing new kit, and form part of the planning and development process and in any event must be fully completed before any processing begins.

To assess the level of risk, a DPIA must consider both the **likelihood of any risk** occurring and the **severity of any consequential harm** caused either to individuals or to society at large should any of the risks occur. A DPIA does not have to completely eradicate risks, but should minimise risks and assess whether or not any remaining risks are justified.

A properly documented DPIA is important for evidencing compliance and should take account of a controller's other express obligations including:

- Article 5: Principles & Accountability
- Article 24: Responsibility of the controller
- Article 25: Data protection by design and default

*(For competent authorities processing personal data subject to the 'Applied LED', the provisions relevant to a DPIA are set out in Article 27 of the 'Applied LED', Regulation 57 of the Regulations and further explanation is provided in Recital 59)*

### Who is responsible for completing a DPIA?

The responsible owner for introducing new or revised service or changes to a new system, process or information asset.

The Data Protection Officer (DPO) must be consulted at the start of the design phase of any new service, process and/or system to seek advice on the need and procedures for completing the DPIA.

### Risks to an individual?

Many requirements of the Applied GDPR including security, appropriate measures, records of processing activities, data protection impact assessments etc., require a consideration of the "**risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing**".

An objective assessment should be undertaken to establish whether the processing operations involve a risk, or in some cases, a high risk, **to the individual**, and the likelihood and severity of that risk.

The following are broad examples of the **risks** to the individual that the processing of data may lead to:

- Physical damage
- Material damage
- Moral damage

This relates in particular to processing in the following 6 areas:

#### 1. Effect on the individual:

- Discrimination
- Identity theft or fraud,
- Financial loss,
- Damage to the reputation,
- Loss of confidentiality of data protected by professional secrecy,
- Unauthorised reversal of pseudonymisation, or
- Any other significant economic or social disadvantage

#### 2. Where data subjects might be **deprived of their rights and freedoms or from exercising control over their personal data**

#### 3. Where **special categories** of personal data are processed:

- Racial or ethnic origin,
  - Political opinions,
  - Religion or philosophical beliefs,
  - Trade-union membership,
  - The processing of genetic data or
  - Data concerning health or sex life or
  - Criminal convictions and offences or
  - Related security measures
4. **Profiling** - where personal aspects are evaluated, in particular analysing or prediction of aspects concerning
  5. Where personal data of vulnerable individuals, in particular of children, are processed;
  6. Where processing involves a **large amount of personal data and affects a large number of data subjects**.

Relevant Recitals:

**Recital 75:** Risks to the Rights and Freedoms of Natural Persons  
**Recital 84:** Data Protection Impact Assessment  
**Recital 89:** Abolishment of Indiscriminate General Notification  
**Recital 90:** Impact Assessment Modalities and Scope  
**Recital 91:** Conditions Necessitating an Impact Assessment  
**Recital 92:** Broader Data Protection Impact Assessments  
**Recital 93:** Data Protection Impact at Public Authorities and Bodies

**Note:**

The Law

According to well-established rules, a public authority must possess the power to carry out what it intends to do.

If not, its action is 'ultra vires', that is, beyond its lawful powers.

It is also necessary that the power is exercised for the purpose for which it was created or is 'reasonably incidental' to the defined purpose.

It is important that the Department is aware of the extent and limitations of our powers and act 'intra vires'.

The approach often adopted by Government to address situations where a disclosure of information is prevented by lack of function (the 'ultra vires' rule), is to create, through legislation, new statutory gateways that provide public sector bodies with the appropriate information disclosure function.

However, unless such legislation explicitly requires that confidential patient/client information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosure and use taking place, for example by obtaining explicit patient/client consent.

Examples of High Risk Processing (this is not an exhaustive list)

Type of processing operation(s) requiring a DPIA	Description	Non-exhaustive examples of existing areas of application
<b>Innovative Technology</b>	<p>Processing involving the use of new technologies, or the novel application of existing technologies (including AI).</p> <p>A DPIA is required for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions) when combined with any other criterion from <a href="#"><sup>7</sup>WP248rev01</a></p>	<ul style="list-style-type: none"> <li>• Artificial intelligence, machine learning and deep learning</li> <li>• Connected and autonomous vehicles</li> <li>• Intelligent transport systems</li> <li>• Smart technologies (including wearables)</li> <li>• Market research involving neuro-measurement (i.e. emotional response analysis and brain activity)</li> <li>• Some IoT applications, depending on the specific circumstances of the processing</li> </ul>
<b>Denial of Service</b>	<p>Decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special- category data.</p>	<ul style="list-style-type: none"> <li>• Credit checks</li> <li>• Mortgage or insurance applications</li> <li>• Other pre-check processes related to contracts (i.e. smartphones)</li> </ul>
<b>Large-Scale Profiling</b>	<p>Any profiling of individuals on a large scale</p>	<ul style="list-style-type: none"> <li>• Data processed by Smart Meters or IoT applications</li> <li>• Hardware/software offering fitness/lifestyle monitoring</li> <li>• Social-media networks</li> <li>• Application of AI to existing process</li> </ul>

<sup>7</sup> European Commission – Guidelines on data Protection Impact Assessment (DPIA) <https://ec.europa.eu/newsroom/article29/items/611236/en>



<b>Biometric Data</b>	<p>Any processing of biometric data for the purpose of uniquely identifying an individual.</p> <p>A DPIA is required for any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion from <a href="#">WP248rev01</a></p>	<ul style="list-style-type: none"> <li>• Facial recognition systems</li> <li>• Workplace access systems/identity verification</li> <li>• Access control/identity verification for hardware/applications (including voice recognition/fingerprint/facial recognition)</li> </ul>
<b>Genetic Data</b>	<p>Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.</p> <p>A DPIA is required for any intended processing operation(s) involving genetic data when combined with any other criterion from <a href="#">WP248rev01</a></p>	<ul style="list-style-type: none"> <li>• Medical diagnosis</li> <li>• DNA testing</li> <li>• Medical research</li> </ul>
<b>Data matching</b>	<p>Combining, comparing or matching personal data obtained from multiple sources</p>	<ul style="list-style-type: none"> <li>• Fraud prevention</li> <li>• Direct marketing</li> <li>• Monitoring personal use/uptake of statutory services or benefits</li> <li>• Federated identity assurance services</li> </ul>
<b>Invisible processing</b>	<p>Processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort (as provided by Article 14.5(b).</p> <p>A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from <a href="#">WP248rev01</a></p>	<ul style="list-style-type: none"> <li>• List brokering</li> <li>• Direct marketing</li> <li>• Online tracking by third parties</li> <li>• Online advertising</li> <li>• Data aggregation/data aggregation platforms</li> <li>• Re-use of publicly available data</li> </ul>



<p><b>Tracking</b></p>	<p>Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.</p> <p>A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from <a href="#">WP248rev01</a></p>	<ul style="list-style-type: none"> <li>• Social networks, software applications</li> <li>• Hardware/software offering fitness/lifestyle/health monitoring</li> <li>• IoT devices, applications and platforms</li> <li>• Online advertising</li> <li>• Web and cross-device tracking</li> <li>• Data aggregation / data aggregation platforms</li> <li>• Eye tracking</li> <li>• Data processing at the workplace</li> <li>• Data processing in the context of home and remote working</li> <li>• Processing location data of employees</li> <li>• Loyalty schemes</li> <li>• Tracing services (tele-matching, tele-appending)</li> <li>• Wealth profiling – identification of high net-worth individuals for the purposes of direct marketing</li> </ul>
<p><b>Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services</b></p>	<p>The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.</p>	<ul style="list-style-type: none"> <li>• Connected toys</li> <li>• Social networks</li> </ul>
<p><b>Risk of physical harm</b></p>	<p>Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.</p>	<ul style="list-style-type: none"> <li>• Whistleblowing/complaint procedures</li> <li>• Social care records</li> </ul>

## Appendix 7: Glossary

Term	Definition
Accountability	Accountability is one of the data protection principles: it makes the controller responsible for complying with the Applied GDPR and able to demonstrate compliance
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, such as facial images or fingerprint data.
Breach	Any failure to meet the requirements of the Data Protection Act and/or the Applied GDPR, an unlawful disclosure of confidential personal information or misuse of personal data and an inappropriate invasion of people's privacy
Caldicott Guardian	A senior person in an organisation responsible for protecting the confidentiality of patient information and enabling appropriate information sharing by providing advice to professionals and staff
Common law	Laws that are based on court or tribunal decisions which govern future decisions on similar cases
Common Law Duty of Confidentiality (CLDC)	<p>This arises when one person discloses information to another, for example, patient to clinician, in circumstances where it is reasonable to expect that the information will be held in confidence. It:</p> <ol style="list-style-type: none"> <li>1. is a legal obligation that is derived from common law;</li> <li>2. is a requirement established either within professional codes of conduct and/or that must be included within relevant employment contracts. It is also linked to disciplinary procedures through both these requirements.</li> </ol> <p>It would also apply where confidential information is received or obtained from another organisation as the data subject would have a reasonable expectation that any recipient would hold it in confidence.</p>
Consent	<p>Consent can be used for a number of different purposes, offering individuals real choice and control. When using consent, organisations need to be clear on why they are getting consent (for example to satisfy confidentiality, medico-legal reasons, or for processing data).</p> <p>Explicit consent requires a positive opt-in and must be evidential.</p> <p>The Applied GDPR sets a high standard for consent. Often consent is not the appropriate legal basis for processing health and care data, and another lawful basis can be found. However, consent may still be required to meet the CLDC.</p>



Controller	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
Cyber threat	The possibility of a malicious attempt to damage or disrupt a computer network or system.

Data Breach Notification	A duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The supervisory authority in the Isle of Man is the Information Commissioner's Office
Data Protection Law 2018	Several legal instruments constitute the "data protection law 2018". Those instruments, and how they are referenced on this site, are:  <b>Legal instrument</b>  Data Protection Act 2018  Data Protection (Application of the GDPR) Order 2018  Adapted text of the EU GDPR in the Annex to the GDPR Order  Data Protection (Application of the LED) Order 2018  The GDPR and LED Implementing Regulations 2018
Data Protection Impact Assessment (DPIA)	A Data Protection Impact Assessment (DPIA) is a method by which a controller can <b>objectively, systematically and comprehensively</b> assess the proposed processing of personal data and identify, and minimise, the risks to an individual when developing a new, or updating an existing, system. The fundamental aim is to weigh the need for, and the potential benefit of, the processing against the impact on individuals. An effective DPIA can provide compliance, financial and reputational benefits, which help demonstrate accountability and assist a controller build trust and confidence with individuals.
Data Protection Officer (DPO)	An independent expert in data protection who helps monitor internal compliance, informs and advises on data obligations including Data Protection Impact Assessments and acts as a point of contact for data subjects and the Information Commissioner's Office
Data Security	Protecting data and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Data Subject	An identified or identifiable natural person.
Duty of Transparency	<p>The Applied GDPR principle of accountability requires that organisations must be able to demonstrate compliance.</p> <p>Part of this involves transparency and the provision of information to subjects – previously referred to as fair processing.</p> <p>A specific requirement of the Applied GDPR is that organisations <u>must</u> include their lawful basis for processing information provided to patients, service users and staff</p>
Explicit Consent	Explicit consent requires a very clear and specific statement of consent. It is unmistakable. It can be given in writing or verbally, or conveyed through another form of communication such as signing. Whilst explicit consent is not required for direct care purposes, it may still be required to comply with other statutory requirements
Genetic Data	Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question
Human Rights Act 2001	The Act makes it unlawful for a public authority to behave in a way which contravenes those rights. This means that all public authorities must ensure that everything they do is compatible with Convention rights unless an Act of Tynwald makes that impossible. People are entitled to expect that public authorities respect their Convention rights.
Implied Consent	<p>Only applies in the context of care provided to individuals (or actions that lead to the provision of care). Implied consent refers to instances where the consent of the individual patient can be implied, without them having to make any positive indication of their wishes, such as giving their verbal agreement for a specific aspect of sharing information to proceed.</p> <p>An example of implied consent would be doctors and nurses sharing CPI during handovers without asking for the patient's consent. Alternatively, a physiotherapist may access the record of a patient who has already accepted a referral before a face-to-face consultation.</p> <p>To use implied consent, organisations must inform patients or service users of how their information may be used when providing services. Typically, this could be included in patient or service user information leaflets about a service, or as transparency information on their website about how the organisation uses personal and health and care data.</p>

Individual Care	<p>Has the same meaning as Direct Care. Both definitions below are taken from "<a href="#">Information: To Share or not to Share? The IG Review 2013</a>".</p> <ol style="list-style-type: none"> <li>1. A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.</li> <li>2. Direct care is provided by health and social care staff working in care teams, which may include doctors, nurses and a wide range of staff on regulated professional registers, including social workers. Relevant information should be shared with them when they have a legitimate relationship with the patient or service user</li> </ol>
Information Commissioner's Office (ICO)	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals
Information Governance (IG)	The term used to describe how organisations and individuals manage and handle data within the health and social care system. In practical terms, IG is about managing and sharing information appropriately.
Joint Controllers or Joint Controllership	<p>Where two or more controllers jointly determine the purposes and means of processing. Joint controllers are not required to have a contract but must have a transparent arrangement that sets out agreed roles and responsibilities for complying with the Applied GDPR</p> <p><b>Note:</b> There is no reference to 'Controllers in common' in the Applied GDPR and must not be used.</p>
Joint Controller Arrangement	Joint controllers are not required to have a contract but must have a transparent arrangement that sets out your agreed roles and responsibilities for complying with the Applied GDPR
Lawful Basis	The principle of accountability requires you to be able to demonstrate that you are complying with the Applied GDPR, and have appropriate policies and processes. This means that you need to be able to show that you have properly considered which lawful basis applies to each processing purpose and can justify your decision
Legal Entity	<p>A lawful or legally standing association corporation, partnership, proprietorship, trust or individual which has legal capacity to:</p> <ul style="list-style-type: none"> <li>• Enter into agreements or contracts</li> <li>• Assume obligations</li> </ul>



	<ul style="list-style-type: none"> <li>• Incur and pay debts</li> <li>• Sue and be sued in its own right, and</li> <li>• To be accountable for illegal activities.</li> </ul>
Legal Obligation	The obligation or duty that is enforced by a court of law
Natural Person	A living human being with certain rights and responsibilities under law
Participating Organisation	Participating organisations are those statutory organisations or other legal entities signed up to a DSA or other organisations contracted by a statutory organisation, which could be a private sector or 3rd sector organisation.
Personal Data	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
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Processing	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
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Reasonable Expectations	What a reasonable person would expect to happen, given the circumstances and information available to them. This is important to consider when relying on implied consent
Records of Processing Activity (RoPA)	Article 30 of the Applied GDPR states that each controller shall maintain a record of processing activities under its responsibilities. The Article details what should be contained in the record
Risk Register	DPIAs require an assessment of risks and measures to help mitigate those risks. A risk register is a tool which can support this by formally capturing the risk, information, the nature, the owner and the mitigation of each risk.

Role Based Access Control (RBAC)	Access to data is dependent on the role of the person, for instance, a medical receptionist would see different information to a consultant.
Special Category Data	Personal data which the Applied GDPR says is more sensitive, and so needs more protection. Such data includes health, genetic, and biometric data.
Statutory Functions	These functions that an organisation is legally required to do as set out in Acts of Tynwald
Subject Access Request (SAR)	Under Article 15 of the Applied GDPR (the right of access) Individuals have a right of access to their personal data. This is commonly referred to as a SAR
Third Party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor (if they process personal data in their own right then they will also become a controller)
Threat	Any circumstance or event with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data and/or denial of service
Transparency Information	Information provided to individuals about the collection and use of their personal data. This must include purposes for processing their personal data, retention periods for that personal data, and who it will be shared with. This must be provided at the time personal data is collected or as soon as practically possible after the collection. This used to be called a privacy notice.