CRYSTAL PEAKS MEDICAL CENTRE

UK GDPR Policy incorporating Data Protection and Security

Document Control

Title of document	UK GDPR Policy Incorporating Data Protection and Security
Author's name	Michelle Smith
Author's job title	Practice Manager
Date	01.11.2011
Review Date	13.03.2013
Next Review Date	13.03.2013
Date of Review	12.01.2015
Reviewed by	Hannah Smith
Next review date	12.01.2016
Reviewed by	Michelle Smith
Date of Review	February 2016
Date of Next Review	February 2017
Date of Review	May 2018
Reviewed by	Michelle Smith
Date of Next Review	May 2019
Date of Review	April 2019
Reviewed by	Michelle Smith
Date of Next Review	April 2020
Date of Review	June 2021
Reviewed by	Hannah Smith
Date of Next Review	June 2022
Distribution	Electronic TOK available to all practice

UK General Data Protection Regulation Policy incorporating Data Protection and Security

Introduction

1.1 Policy statement

The UK General Data Protection Regulation (UK GDPR herein) came into force on 1 January 2021 and is incorporated in the Data Protection Act 2018 (DPA18) at part 2. The UK GDPR applies to all organisations in the UK (with the exception of law enforcement and intelligence agencies) and Crystal Peaks Medical Centre must be able to demonstrate compliance at all times. Understanding the requirements of the UK GDPR will ensure that the personal data of both staff and patients is protected accordingly.

1.2 Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have regarding individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

1.3 KLOE

The Care Quality Commission would expect any primary care organisation to have a policy to support this process and this should be used as evidence of compliance against CQC Key Lines of Enquiry (KLOE).

Specifically, Crystal Peaks Medical Centre will need to answer CQC key questions on "Safe" and "Well-Led".

The following is the CQC definition of Safe:

By safe, we mean people are protected from abuse and avoidable harm. *Abuse can be physical, sexual, mental or psychological, financial, neglect, institutional or discriminatory abuse.*

CQC KLOE S3	Do staff have all the information they need to deliver safe care and treatment to people?
S3.3	When people move between teams, services and organisations (which may include at referral, discharge,

	transfer and transition), is all the information needed for their ongoing care shared appropriately, in a timely way and in line with relevant protocols?
S3.4	How well do the systems that manage information about people who use services support staff, carers and partner agencies to deliver safe care and treatment? (This includes coordination between different electronic and paper-based systems and appropriate access for staff to records.)

The following is the CQC definition of Well-Led

By well-led, we mean that the leadership, management and governance of the organisation assures the delivery of high-quality and person-centred care, supports learning and innovation and promotes an open and fair culture.

CQC KLOE W3	Is there a culture of high-quality, sustainable care?
W3.5	Does the culture encourage openness and honesty at all levels within the organisation, including with people who use services, in response to incidents? Do leaders and staff understand the importance of staff being able to raise concerns without fear of retribution and is appropriate learning and action taken as a result of concerns raised?
CQC KLOE W6	Is appropriate and accurate information being effectively processed, challenged and acted on?
W6.7	Are there robust arrangements (including appropriate internal and external validation) to ensure the availability, integrity and confidentiality of identifiable data, records and data management systems, in line with data security standards? Are lessons learned when there are data security breaches?

1.4 Training and support

The organisation will provide guidance and support to help those to whom it applies to understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

2 Scope

2.1 Who it applies to

This document applies to all employees, partners and directors of the organisation. Other individuals performing functions in relation to the organisation, such as agency workers, locums and contractors, are encouraged to use it.

Furthermore, it also applies to clinicians who may or may not be employed by the organisation but who are working under the Additional Roles Reimbursement Scheme (ARRS).[1]

2.2 Why and how it applies to them

All personnel at Crystal Peaks Medical Centre have a responsibility to protect the information they process. This document has been produced to enable all staff to understand their individual and collective responsibilities in relation to the UK GDPR.

3 Definition of terms

3.1 Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) sets out the framework for data protection law in the UK. It sits alongside and supplements the UK General Data Protection Regulation (UK GDPR).[2]

3.2 Data protection by design and default

Data protection by design and default means putting in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights.[3]

3.3 Data Protection Officer

An expert on data privacy, working independently to ensure compliance with policies and procedure

3.4 Data controller

The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data[4]

3.5 Data processor

A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller[4]

[1] Network Contract Directed Enhanced Service (DES) Contract specification 2020/21 - PCN Requirements and Entitlements (Annex B P67)
[2] ICO About the DPA 2018
[3] ICO Guide to the UK General Data Protection Regulation
[4] Article 4 UK GDPR

3.6 Data subject

The identified or identifiable living individual to who personal data relates[5]

3.7 UK General Data Protection Regulation (UK GDPR)

The UK GDPR sets out the key principles, rights and obligations for most processing of personal data in the UK.[3]

3.8 Personal data

Information that relates to an identified or identifiable individual[6]

3.9 Processing

Any operation or set of operations that 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

3.10 Pseudonymisation

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual.[6]

3.11 Recipient

The entity to which personal data is disclosed

4 Introduction of the UK GDPR

4.1 Background

The UK GDPR was introduced on 1 January 2021 and is largely based on the EU GDPR which had applied in the UK since 25 May 2018.

4.2 UK GDPR and DPA18

The UK GDPR is incorporated in the DPA18 at Part 2.

[5] ICO Definitions
[6] ICO What is personal data

5 Data protection by design and default

5.1 Data protection by design

Data protection by design is ultimately an approach that ensures that privacy and data protection issues are considered at the design phase of any system, service, product or process and then throughout the lifecycle.[3]

Crystal Peaks Medical Centre will demonstrate data protection by design by:

- Conducting a data protection impact assessment (DPIA)
- Ensuring there are privacy notices on the website and in the waiting rooms which are written in simple, easy-to-understand language
- Adhering to Articles 25(1) and 25(2) of the UK GDPR[7]
- Adhering to Section 6.1 of this policy

Data protection by design is a legal requirement.

5.2 Data protection by default

Data protection by default is an approach that ensures that data is processed only for the achievement of a specific purpose.[3]

Crystal Peaks Medical Centre will demonstrate data protection by default by:

- Processing data only for the purpose(s) intended
- Ensuring consent is obtained from the data subject prior to data being processed
- Providing patients access to their data on request (Subject Access Requests)
- Ensuring patients consent to access of their data by third parties
- Processing data in a manner that prevents data subjects being identified unless additional information is provided (using a reference number as opposed to names – pseudonymisation)
- Processing data in accordance with section 6.2 of this policy

Through effective data protection Crystal Peaks Medical Centre will remain compliant with the UK GDPR.

6 Roles of data controllers and processors

6.1 Data controller

At Crystal Peaks Medical Centre, the role of the data controller is to ensure that data is processed in accordance with Article 5 of the UK GDPR. He/she should be able to demonstrate compliance and is responsible for making sure that data is:[8]

[7] Article 25 GDPR

- Processed lawfully, fairly and in a transparent manner in relation to the data subject
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data, which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- 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

The data controller at Crystal Peaks Medical Centre is Michelle Smith, Practice Manager. They are responsible for ensuring that all data processors comply with this policy and the UK GDPR.

6.2 Data processor

Data processors are responsible for the processing of personal data on behalf of the data controller. Processors must ensure that processing is lawful and that at least one of the following applies:[9]

- The data subject has given consent to the processing of his/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 to which the data controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or 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 data controller
- Processing is necessary for the purposes of the legitimate interests pursued by the data 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

At Crystal Peaks Medical Centre, all staff are classed as data processors as their individual roles will require them to access and process personal data.

---

[8] Article 5 Principles relating to processing of personal data

[9] Article 6 Lawfulness of processing

7 Data subjects' rights

7.1 Overview

All data subjects have the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

7.2 Right to be informed

In accordance with Articles 13 and 14 of the UK GDPR Crystal Peaks Medical Centre is obliged to advise data subjects of the purposes for processing their data, the retention periods for the data and who this data will be shared with. This is referred to as privacy information.

7.3 Right of access

Crystal Peaks Medical Centre ensures that all patients are aware of their right to access their data and has privacy notices displayed in the following locations:

- Waiting room
- Organisation website

To comply with the UK GDPR, all organisation privacy notices are written in a language that is understandable to all patients and meet the criteria detailed in Articles 12, 13 and 14 of the UK GDPR.

The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them. In addition, data subjects can authorise third party access, e.g., for solicitors and insurers, under the UK GDPR.

7.4 Right to rectification

In accordance with Article 16 of the UK GDPR, data subjects have the right to have inaccurate personal data rectified and/or incomplete personal data completed. At Crystal Peaks Medical Centre, should a clinician enter a diagnosis that is later proved incorrect, the medical record should retain both the initial diagnosis and the subsequent accurate diagnosis with text to make it clear that the diagnosis has been updated.

Patients can exercise their right to challenge the accuracy of their data and request that this is corrected. Should a request be received, the request should state the following:

- What is believed to be inaccurate or incomplete
- How this organisation should correct it
- If able to, provide evidence of the inaccuracies

A request can be verbal or in writing and the Information Commissioner's Office (ICO) recommends that any request is followed up in writing as this will allow the requestor to explain their concerns, give evidence and state the desired solution. Additionally, this will also provide clear proof of the requestor's actions, should they decide to challenge this organisation's initial response.

Detailed guidance from the ICO can be accessed here.

7.5 Right to erasure

In accordance with Article 17 of the UK GDPR, data subjects have the right to have personal data erased (this is also referred to as the right to be forgotten). This right permits a data subject to request personal data is deleted in situations where there is no compelling reason to retain the data.

The BMA states: "Whilst it will be extremely rare for information to be deleted from medical records, it is established practice that corrections or amendments can be made; however, the original information, along with an explanation as to why information has been corrected or amended, must remain as an audit trail."

Crystal Peaks Medical Centre will adhere to the BMA guidance.

Where Crystal Peaks Medical Centre has shared information with a third party, there is an obligation to inform the third party about the data subject's request to erase their data providing it is achievable and reasonably practical to do so. Detailed guidance can be accessed here.

7.6 Right to restrict processing

In accordance with Article 18 of the UK GDPR, individuals have the right to restrict the processing of their personal data. This applies in certain circumstances, with the aim being to enable the individual to limit the way an organisation processes (uses) their data. This right can be used as an alternative to the right to erasure.

7.7 Right to data portability

The right to data portability permits data subjects to receive and reuse their personal data for their own purposes and across different services.

7.8 Right to object

In accordance with Article 21 of the UK GDPR, individuals have the right to object to the processing of their personal data at any time. At Crystal Peaks Medical Centre, individuals are requested to provide specific reasons why they object to the processing of their data. If the reasons are not an absolute right, Crystal Peaks Medical Centre can refuse to comply. See the ICO guidance for detailed information.

7.9 Rights in relation to automated decision making and profiling

In accordance with Article 22 of the UK GDPR, Crystal Peaks Medical Centre is not permitted to make solely automated decision making. This includes profiling.

8 Subject access requests

8.1 Recognising subject access requests

At Crystal Peaks Medical Centre, data subjects are encouraged to use the subject access request (SAR) form which is included in the Access to medical records policy. All staff must note that the ICO state:

"An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data."

Any requests not using the SAR form, must be processed.

8.2 Responding to a subject access request

In accordance with the UK GDPR, data controllers must respond to all data subject access requests within one month of receiving the request. It is the guidance of the ICO that a universal approach is applied and a 28-day response time implemented.[10] At Crystal Peaks Medical Centre, the 28 day time frame for response applies.

In the case of complex or multiple requests, the data controller may extend the response time by a period of two months. In such instances, the data subject must be informed and the reasons for the delay explained.

Should the request involve a large amount of information, the data controller will ask the data subject to specify what data they require before responding to the request. Data controllers are permitted to 'stop the clock' in relation to the response time until clarification is received.

8.3 Fees

Under the UK GDPR, Crystal Peaks Medical Centre is not permitted to charge data subjects for initial access; this must be done free of charge. In instances where

[10] ICO Right of access

requests for copies of the same information are received or requests are deemed "unfounded, excessive or repetitive", a reasonable fee may be charged. However, this does not permit the organisation to charge for all subsequent access requests.[11]

The fee is to be based on the administrative costs associated with providing the requested information.

8.4 Verifying the subject access request

It is the responsibility of the data controller to verify all requests from data subjects using reasonable measures.

The use of the organisation's Subject Access Request (SAR) form supports the data controller in verifying the request. In addition, the data controller is permitted to ask for evidence to identify the data subject, usually by using photographic identification, i.e., driving licence or passport.

8.5 Supplying the requested information

The decision on what format to provide the requested information in should take into consideration the circumstances of the request and whether the individual can access the data in the format provided.

Should an individual submit a SAR electronically, Crystal Peaks Medical Centre will reply in the same format (unless the data subject states otherwise).

8.6 Third party requests

At Crystal Peaks Medical Centre, the data controller must be able to satisfy themselves that the person requesting the data has the authority of the data subject.

The responsibility for providing the required authority rests with the third party and is usually in the form of a written statement or consent form, signed by the data subject. A standard consent form has been issued by the BMA and Law Society of England and Wales and Crystal Peaks Medical Centre will request that third parties complete this form.

8.7 Requests from solicitors

At Crystal Peaks Medical Centre], requests are received from third parties such as solicitors. It is the responsibility of the third party to provide evidence that they are permitted to make a SAR on behalf of their client. If concern or doubt arises, Crystal Peaks Medical Centre will contact the patient to explain the extent of disclosure sought by the third party.

[11] BMA Guidance – Access to health records

Crystal Peaks Medical Centre can then provide the patient with the data as opposed to directly disclosing it to the third party. The patient is then given the opportunity to review their data and decide whether they are content to share the information with the third party.

8.8 Requests from insurers

SARs are not appropriate should an insurance company require health data to assess a claim. The correct process for this at Crystal Peaks Medical Centre is for the insurer to use the Access to Medical Reports Act 1988 (AMRA) when requesting a GP report.

The following fees are applicable:[12]

- GP report for insurance applicants £104.00
- GP supplementary report £27.00

8.9 Refusing to comply with a SAR

Crystal Peaks Medical Centre will only refuse to comply with a SAR where exemption applies or when the request is manifestly unfounded or manifestly excessive. In such situations, the data controller will inform the individual of:

- The reasons why the SAR was refused
- Their right to submit a complaint to the ICO
- Their ability to seek enforcement of this right through the courts

Each request must be given careful consideration and should Crystal Peaks Medical Centre refuse to comply, this must be recorded and the reasons for refusal justifiable.

9 Data breaches

9.1 Data breach definition

A data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data.[13]

Examples of data breaches include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a data controller or processor
- Sending personal data to an incorrect recipient
- Loss or theft of computer devices containing personal data
- Alteration of personal data without permission
- Loss of availability of personal data

[12] BMA Guidance – Fees for insurance reports and certificates
[13] ICO – Personal data breaches

Examples of data breaches can be found on the ICO website.

9.2 Reporting a data breach

At Crystal Peaks Medical Centre, should any member of staff become aware of a data breach, they are, where possible, to contain the breach and advise Management or Senior Partner immediately.

When determining whether Crystal Peaks Medical Centre needs to report the data breach to the ICO, this decision is to be based on whether or not the breach is a high risk to an individual's rights and freedoms. If this is deemed to be the case, then the ICO will need to be notified.

Whatever decision is made, Crystal Peaks Medical Centre must be able to justify the decision.

Breaches are to be reported to the ICO without undue delay or within 72 hours of becoming aware of the breach. Crystal Peaks Medical Centre will report the breach using the Data Security and Protection Incident Reporting Tool.

Failure to report a breach can result in a fine of up to £8.7m. It is therefore imperative that there are effective processes in place at Crystal Peaks Medical Centre to detect, investigate and report breaches accordingly.

The data controller is to ensure that all breaches at Crystal Peaks Medical Centre are recorded. Article 33 of the UK GDPR outlines the requirements which include:

- Recording the facts pertaining to the breach
- The effects the breach has had on individuals or organisations
- Any remedial action(s) that have been completed
- The cause of the breach i.e., system or human error
- Considering what system or process changes may be required to prevent future incidences

9.3 Notifying a data subject of a breach

The data controller must notify a data subject of a breach that has affected their personal data without undue delay. If the breach is high risk (i.e., a breach that is likely to have an adverse effect on an individual's rights or freedoms), then the data controller is to notify the individual before they notify the ICO.

The primary reason for notifying a data subject of a breach is to afford them the opportunity to take the necessary steps in order to protect themselves from the effects of a breach.

When the decision has been made to notify a data subject of a breach, the data controller at Crystal Peaks Medical Centre is to provide the data subject with the following information in a clear, comprehensible manner:

- The circumstances surrounding the breach
- The details of the person who will be managing the breach
- Any actions taken to contain and manage the breach
- Any other pertinent information to support the data subject

10 Consent

10.1 Appropriateness

The UK GDPR states that consent must be unambiguous and requires a positive action to "opt in" and it must be freely given. Data subjects have the right to withdraw consent at any time.

10.2 Obtaining consent

Consent is one of the lawful bases of processing and is appropriate if data processors are in a position to "offer people real choice and control over how their data is used".[14] If it is deemed appropriate to obtain consent, the following must be explained to the data subject:

- Why the organisation wants the data
- How the data will be used by the organisation
- The names of any third party data controllers with whom the data will be shared
- Their right to withdraw consent at any time

All requests for consent are to be recorded, with the record showing:

- The details of the data subject consenting
- When they consented
- How they consented
- What information the data subject was told

Consent is to be clearly identifiable and separate from other comments entered into the healthcare record. At Crystal Peaks Medical Centre, it is the responsibility of the data controller Michelle Smith, Practice Manager to demonstrate that consent has been obtained. Furthermore, the data controller must ensure that data subjects (patients) are fully aware of their right to withdraw consent and must facilitate withdrawal as and when it is requested.

10.3 Parental consent

The DPA 2018 states that parental consent (in relation to personal data) is required for a child under the age of 13. Additionally, the principle of Gillick competence remains

[14] ICO Consent

unaffected and parental consent is not necessary when a child is receiving counselling or preventative care.

For further information refer to the Consent Policy.

11 Data mapping and Data Protection Impact Assessments

11.1 Data mapping

Data mapping is a means of determining the information flow throughout an organisation. Understanding the why, who, what, when and where of the information pathway will enable Crystal Peaks Medical Centre to undertake a thorough assessment of the risks associated with current data processes.

Effective data mapping will identify what data is being processed, the format of the data, how it is being transferred, if the data is being shared and where it is stored (including off-site storage if applicable).

Annex A details the process of data mapping at Crystal Peaks Medical Centre.

11.2 Data mapping and the Data Protection Impact Assessment

Data mapping is linked to the Data Protection Impact Assessment (DPIA) and, when the risk analysis element of the DPIA process is undertaken, the information ascertained during the mapping process can be used.

Data mapping is not a one person task. All staff at Crystal Peaks Medical Centre will be involved in the mapping process thus enabling the wider gathering of accurate information.

11.3 Data Protection Impact Assessment

The DPIA is the most efficient way for Crystal Peaks Medical Centre to meet its data protection obligations and the expectations of its data subjects. DPIAs are also commonly referred to as Privacy Impact Assessments or PIAs.

In accordance with Article 35 of the UK GDPR, a DPIA should be undertaken where:

- A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks

- Extensive processing activities are undertaken, including large scale processing of personal and/or special data

DPIAs are to include the following:

- A description of the processing operations, including the purpose of processing
- An evaluation of the need for the processing in relation to the purpose
- An assessment of the associated risks to the data subjects
- Existing measures to mitigate and control the risk(s)
- Evidence of compliance in relation to risk control

It is considered best practice to undertake DPIAs for existing processing procedures to ensure that Crystal Peaks Medical Centre meets its data protection obligations. DPIAs are classed as “live documents” and processes should be reviewed continually. As a minimum, a DPIA should be reviewed every three years or whenever there is a change in a process that involves personal data.

11.4 Data Protection Impact Assessment process

The DPIA process is illustrated in diagrammatic form below:

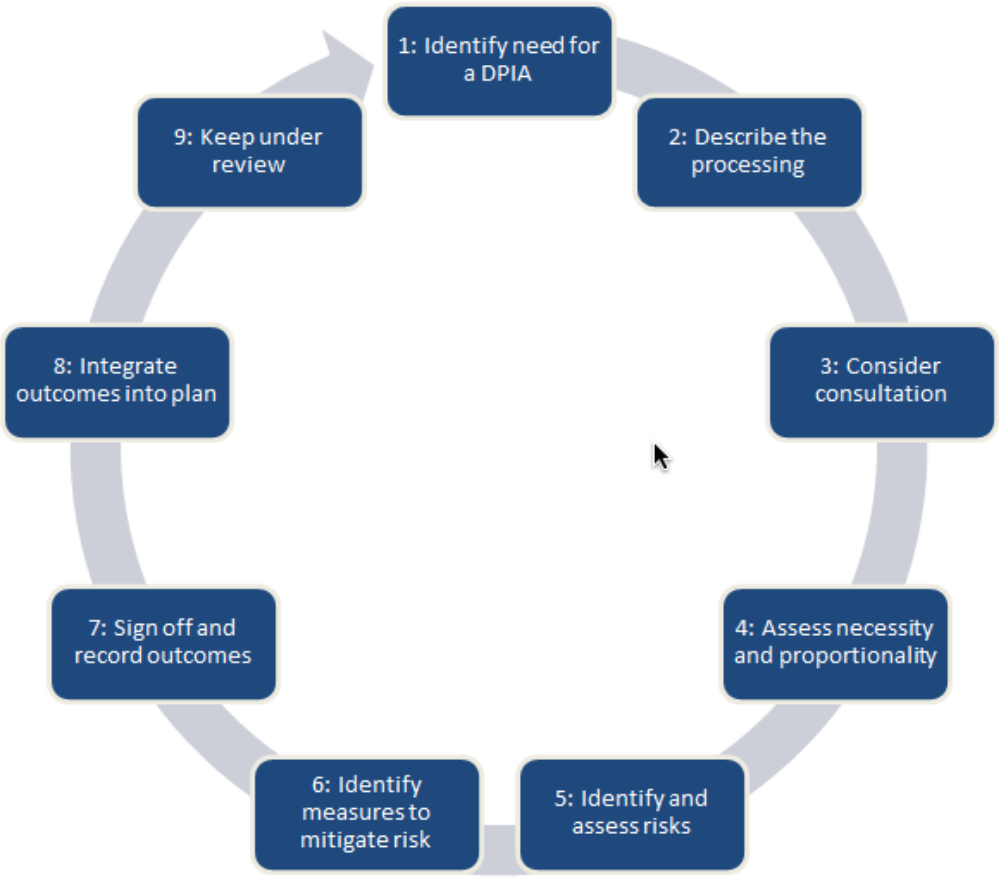

Image source: ico.org.uk

Annex B provides a template that is to be used to carry out a DPIA at Crystal Peaks Medical Centre.

12 Summary

Given the complexity of the UK GDPR, all staff at Crystal Peaks Medical Centre must ensure that they fully understand the requirements within the regulation. Understanding the regulation will ensure that personal data at Crystal Peaks Medical Centre remains protected and the processes associated with this data are effective and correct.

Annex A – The data mapping process

WHY is personal data processed?	
Personal data is defined as "any information relating to an 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".[15]	
Personal data may be used for the following reasons:	
Staff administration	**Patient records**
• Contact details • NOK details • Contracts, DBS applications • Pay, tax, pensions etc. • Application forms for training etc. • Use of IT • Minutes of meetings • Complaints	• Contact details • Health records • NOK details • Referrals • Prescriptions • Online service/practice apps • PPG membership, minutes etc. • Complaints
List the reasons why personal data is processed:	
WHO – whose personal data is processed?	
Having identified why personal data is processed, use those reasons to determine whose personal data is processed.	
Personal data may be processed for the following data subjects:	
Staff	**Patients**
• Current/former • Locums/temps/consultants • Potential employees • Volunteers • CCG/regional staff	• Current/previous • Carers/relatives/guardians • Third party representatives
Contractors/suppliers	**Other**
• Estates • Gardens • Pharmacy • Equipment servicing/repair	• Sales representatives • Guest speakers • Trainers
List whose personal data is processed:	

[15] GDPR Article 4 Definitions

WHAT personal data is processed?	
Having identified why and whose personal data is processed, use those reasons to determine what personal data is processed. The source of the data and the legal basis (why it was provided) must also be recorded.	
Types of personal data that may be processed:	
Staff	**Patients**
• Name/address/NOK • Email/phone number etc. • Occupational health information • Training records • Employment information/ appraisals etc. • ID verification (passport/driving licence etc.)	• Name/address/NOK • Email phone number etc. • Healthcare information • ID verification (passport/driving licence etc.)
Source	**Legal basis**
• Data subject • Third party • Other (specify)	• Legal obligation/lawful function • Consent • Contract related • Legitimate interest of the data controller

List what personal data is processed:		
Data type	**Source**	**Legal basis**

WHEN is personal data processed?	
Having identified why, whose and what personal data is processed, use those reasons to determine when personal data is processed. This includes obtaining, disclosing and deleting data.	
Types of personal data that may be processed:	
Staff	**Patients**
Receiving, transferring or updating the following: • Name/address/NOK • Email/phone number etc. • Occupational health information • Training records • Employment information/ appraisals etc. • ID verification (passport/driving	**Receiving, transferring or updating the following:** • Name/address/NOK • Email/phone number etc. • GP2GP/medical records • Results, letters etc. • ID verification (passport/driving licence etc.)

licence etc.)	
Sharing and disclosure	**Sharing and disclosure**
• Appraisal • References • Awards and recommendations • Occupational health information • Incident reports/forms • Business cases • Insurance and banking	• Referrals • Results • Letters to other service providers
Retention	**Retention**
• In accordance with the current retention schedule	• In accordance with the current retention schedule

List when personal data is processed:		
Obtained/updated	**Disclosure (with whom and why)**	**Retention (how long & IAW retention schedule)**

WHERE is personal data processed?
Having identified why, whose, what and when personal data is processed, use those reasons to determine where personal data is processed. The source of the data and the legal basis (why was it provided) must also be recorded.

Types of personal data that may be processed:	
Staff	**Patients**
• Name/address/NOK • Email/phone number etc. • Occupational health information • Training records • Employment information/ appraisals etc. • ID verification (passport/driving licence etc.)	• Name/address/NOK • Email/phone number etc. • Healthcare information • ID verification (passport/driving licence etc.)

Manual records	**Electronic records**	**IT system**
• Lloyd George • Staff files • Hard copies of prescriptions etc.	• Locally established databases • SystmOne • EMIS Web • Vision	• Fixed • Portable (laptops) • Remote servers • Intranet

Manual:
Electronic records:
IT system:

Aligning the data – Use the table below to create a data record								
WHY	**WHO**	**WHAT**			**WHEN**			**WHERE**
		Type	**Source**	**Legal basis**	**Obtained/ updated**	**Disclosure (who and why)**	**Retention**	
Patient records	Current patient	Healthcare record	Individual/ third party	Legitimate interests – provision of healthcare services	Upon registration	Referrals to NHS hospital trusts for specialist care if necessary	10 years after death (Records Management Code of Practice for Health & Social Care 2016) Sent to the Health Authority.	Electronic records – SystmOne Manual record – Lloyd George wallet – Locked files in reception area

Annex B – The Data Protection Impact Assessment

This document is to be used to conduct a DPIA at Crystal Peaks Medical Centre.

Step 1 – Determining the need

Does the process involve any of the following:	YES	NO
The collection, use or sharing of existing data subjects' health information?		
The collection, use or sharing of additional data subjects' health information?		
The use of existing health information for a new purpose?		
The sharing of data subjects' health information between organisations?		
The linking or matching of data subjects' health information that is already held?		
The creation of a database or register which contains data subjects' health information?		
The sharing of data subjects' health information for the purpose of research or studies (regardless of whether the information is anonymised)?		
The introduction of new practice policies and protocols relating to the use of data subjects' personal information?		
The introduction of new technology in relation to the use of data subjects' personal information, i.e., new IT systems, phone lines, online access, etc?		
Any other process involving data subjects' health information that presents a risk to their "rights and freedoms"?		

If the answer is yes to one or more of the above questions, a DPIA is required. Proceed to Step 2.

Step 2 – Assessing the risks

Information collection – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject	
What information is being collected and how?	
Where is the information being collected from and why?	
How often is the information being collected?	
What is the purpose of using the information?	
When and how will the information be processed?	
Is the use of the information linked to the reason(s) for the information being collected?	
What is the process for ensuring the accuracy of data?	
What are the consequences if data is inaccurate?	
How will processes ensure that only extant data will be disclosed?	
What security processes are in place to protect the data?	
What controls are in place to safeguard only authorised access to the	

data?	
How is data transferred; is the process safe and effective?	
What processes are in place for data subject access?	
How can data subjects verify the lawfulness of the processing of data held about them?	
How do data subjects request that inaccuracies are rectified?	
Will information be shared outside the organisation; are data subjects made aware of this?	
Why will this information be shared? Is this explained to data subjects?	
Are there robust procedures in place for third party requests which prevent unauthorised access?	
What are the retention periods associated with the data?	
What is the disposal process and how is this done in a secure manner?	
Where is data stored? If data is moved off-site, what is the process; how can data security be assured?	

Step 3 – Risk mitigation

Information collection – The risk
Personal data is collected without reason or purpose – increased risk of disclosure.
Information collection – The mitigation
The reasons for data collection must be clearly stated and all personnel must understand why the data has been collected.
Information use – The risk
Personal data is used for reasons not explained to, or expected by, the data subjects.
Information use – The mitigation
Clearly explain and display to data subjects how their information will be used. Data-sharing requires a positive action, i.e., opting in, not opting out.
Information attributes – The risk
Data is inaccurate or not related to the data subject.
Information attributes – The mitigation
Make sure robust procedures are in place to ensure the data held about data subjects is accurate, up to date and reflects the requirements of the data subject for which it was intended.

Information security – The risk
Unauthorised access to data due to a lack of effective controls or lapses of security/procedure.
Information security – The mitigation
Ensure that staff are aware of the requirement to adhere to the organisation's security protocols and policies; conduct training to enhance current controls.
Data subject access – The risk
Data subjects are unable to access information held about them or to determine if it is being processed lawfully.
Data subject access – The mitigation
Ensure that data subjects are aware of access to online services and know the procedure to request that information held be amended to correct any inaccuracies.
Information disclosure – The risk
Redacting information before disclosure might not prevent data subjects being identified – i.e., reference to the data subject may be made within the details of a consultation or referral letter.
Information disclosure – The mitigation
Make sure the policy for disclosure is robust enough to ensure that identifying information is removed.
Retention of data – The risk

Data is retained longer than required or the correct disposal process is not adhered to.
Retention of data – The mitigation
Ensure that practice policies and protocols clearly stipulate data retention periods and disposal processes. Review and update protocols and policies and, if necessary, provide training for staff to ensure compliance.

Step 4 – Recording the DPIA

An **example** of a DPIA report is shown overleaf.

Step 5 – Reviewing the DPIA

The review process is detailed in the report.

Data Protection Impact Assessment Report	

Practice name	**[Insert organisation name]**
Data controller	**[Insert name of controller]**
Date of assessment	**[Insert date]**
Process assessed	**[Referral process]**

Overview:

[Insert organisation name] currently adheres to internal policies and national legislation and guidance for all processes that involve personal data. To ensure that the practice is compliant with the UK GPDR, a review of all processes is being undertaken.

The need:

Having completed Step 1 of the DPIA, when asked "Does the process involve any of the following", this question merited a "yes" response: The sharing of data subjects' health information between organisations.

The organisation is frequently required to share data subjects' personal data – more specifically, personal details and healthcare between organisations – that is the sharing of data between [insert organisation name] and [NHS hospital trusts] in [state area]. This is a requirement to ensure that data subjects receive the necessary care and treatment commensurate with their clinical condition(s).

Assessing the risk:

Information collection – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject	
What information is being collected and how?	Personal details, healthcare information
Where is the information being collected from and why?	Data subjects and IT system
How often is the information being collected?	During consultations, which are on an as-needed basis
Information use – Is the data obtained for specified, explicit and legitimate purposes?	
What is the purpose for using the information?	To enable the provision of effective healthcare treatment
When and how will the information be processed?	Recorded during consultations onto the EMIS Web clinical system
Is the use of the information linked to the reason(s) for the information being	Yes

collected?	
Information attributes – Personal data shall be accurate and, where necessary, kept up to date	
What is the process for ensuring the accuracy of data?	Asking the data subject to confirm details and ensuring the correct patient record is used when recording the information
What are the consequences if data is inaccurate?	Incorrect patient record updated; delay in treatment and or referral; potentially adverse impact on patient health
How will processes ensure that only extant data will be disclosed?	Only that information which is pertinent to the referral will be used; this is extracted onto medical templates using the IT system
Information security – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	
What security processes are in place to protect the data?	Only authorised users can access the data. Staff must adhere to the NHS policy for the use of IT equipment
What controls are in place to safeguard only authorised access to the data?	Regular audits of access to healthcare records. All users have an individual log-on and the system is password restricted
How is data transferred? Is the process safe and effective?	The data is transferred electronically using end-to-end encryption
Data subject access – Personal data shall be accurate and, where necessary, kept up to date	
What processes are in place for data subject access?	Data subjects can access limited information using online services or by submitting a SAR
How can data subjects verify the lawfulness of the processing of data held about them?	By accessing their records and viewing how information has been processed
How do data subjects request that inaccuracies are rectified?	Data subjects can request that information held about them be changed by asking for an appointment with the data controller
Information disclosure – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	
Will information be shared outside the practice? Are data subjects made aware of this?	Yes, the practice privacy policy details this information
Why will this information be shared? Is this explained to data subjects?	Yes, to facilitate the necessary examination and treatment of data

	subjects
Are there robust procedures in place for third party requests which prevent unauthorised access?	Yes, authority must be provided by the third party who also included either a written statement or consent form, signed by the data subject
Retention of data – Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed	
What are the retention periods associated with the data?	GP records are retained for a period of 10 years following the death of a patient
What is the disposal process and how is this done in a secure manner?	At the end of the retention period, the records will be reviewed and if no longer needed then destroyed
Where is data stored? If data is moved off-site, what is the process? How can data security be assured?	Patient data is stored electronically on the IT system (EMIS Web) and hard copies of patient records (if held) are stored in the administration office, which can only be accessed by authorised personnel

To assess the risk of this process, this risk matrix was used:

Probability	Severity of Impact/Consequences		
	Minor	Moderate	Major
Frequent	Medium	High	High
Likely	Low	Medium	High
Remote	Insignificant	Low	Medium

The risk for this process has been recorded in the risk register which details the mitigating actions taken to reduce the risk. The register is shown overleaf.

REF #	DATE	RISK	RISK SCORE			OWNER	MITIGATING ACTION(S)	SCORE POST ACTION(S)			PROGRESS	STATUS	DATE CLOSED
			Probability	Impact	Status			Probability	Impact	Status			
PI01/18	01/02/18	Data subjects are unaware that their data is being shared with other organisations i.e. hospitals	Likely	Major		I N Pain (PM)	PM to produce statement for website, poster for waiting room explaining the need to share data. Draft and implement a policy for positive opt-in actions for data sharing.	Likely	Minor		Statement written and uploaded. Waiting Rm poster in progress. Policy drafted pending approval.	Ongoing	

Review requirements

The referral process is fundamental to effective patient healthcare. The process is to be continually monitored to assess the effectiveness of the process; this can be achieved through internal audit.

This DPIA is to be reviewed when there are changes to the referral process (no matter how minor they may seem).

Mandatory review date: [insert review date]

Signature:

[Insert name]

[Position]

[Date]

[Version] – [i.e., Version 1.0 – Reviser – I N Pain – Document Created]