College Health Ltd

General Data Protection Regulation (GDPR) Policy

College Health Ltd

March 2019

CH-G067

Tilbury Chadwell Locality

Commonwealth Health Centre

Tilbury Health Centre

Chadwell Medical Centre

Dilip Sabnis Health Centre

Grays Locality

Thurrock Health Centre

Oddfellows Hall Health Centre

St Clements Health Centre

Document Version, Revision and Approval History

Document Title	General Data Protection Regulation Policy V2
Document Reference Number	CH-G067
Author's Name	Sharon Hogarth
Document Status	V.1
Authorisation By	Dr P Mallik
Practice Manager	Sharon Hogarth
Issue Date	March 2019
Replaces	May 2018
Next Review Date	March 2020
Distribution	All Staff

Publication History

If you are reading this in paper format, please check this is the latest version.
The latest versions of all Policies can be accessed on the shared drive.
In line with the Environmental Management Policy, if you are about to print this document, please consider whether you really need to.

Confidentiality Notice

Version	Date	Version Created By	Version Approved By	Comments
2	22.3.19	Sharon Hogarth	Dr Pro Mallik	

Table of contents

1 Introduction

1.1 Policy statement

1.2 Status

1.3 Training and support

2 Scope

2.1 Who it applies to

2.2 Why and how it applies to them

3 Definition of terms

3.1 Data Protection Bill

3.2 Data Protection Officer

3.3 Data Protection Authority

3.4 Data Controller

3.5 Data Processor

3.6 Data Subject

3.7 Personal data

3.8 Processing

3.9 Recipient

4 The GDPR

4.1 Background

4.2 NHS Digital

4.3 Aim of the GDPR

4.4 Brexit and the GDPR

4.5 GDPR and DPA18

5 Roles of data controllers and processors

5.1 Data controller

5.2 Data processor

6 Access

6.1 Data subject's rights

6.2 Fees

6.3 Responding to a data subject access request

6.4 Verifying the subject access request

6.5 E-requests

6.6 Third-party requests

7 Data breaches

7.1 Data breach definition

7.2 Reporting a data breach

7.3 Notifying a data subject of a breach

8 Data erasure

8.1 Erasure

8.2 Notifying third parties about data erasure requests

9 Consent

9.1 Appropriateness

9.2 Obtaining consent

9.3 Parental consent

10 Data mapping and Data Protection Impact Assessments

10.1 Data mapping

10.2 Data mapping and the Data Protection Impact Assessment

10.3 Data Protection Impact Assessment

10.4 DPIA process

11 Summary

Annex A - The data mapping process

Annex B - The Data Protection Impact Assessment

Annex C - GDPR checklist

1 Introduction

1.1 Policy statement

The EU General Data Protection Regulation (GDPR herein) came into force on 25th May 2018; the Data Protection Act 2018 (DPA 2018) is to be read in conjunction with the GDPR. The GDPR applies to all EU member states and College Health Ltd must be able to demonstrate compliance at all times and also understanding of the requirements of the GDPR, will ensure that personal data of both staff and patients is protected accordingly.

1.2 Status

This document and any procedures contained within it are contractual and therefore form part of your contract of employment. Employees will be consulted on any modifications or change to the document's status.

1.3 Training and support

The practice will provide guidance and support to help those to whom it applies 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 practice. Other individuals performing functions in relation to the practice, such as agency workers, locums and contractors, are encouraged to use it.

2.2 Why and how it applies to them

Personnel at all College Health Surgeries 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 GDPR.

The practice 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 in regard to the individual protected characteristics of those to whom it applies.

3 Definition of terms

3.1 Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) is a complete data protection system, covering general data, law enforcement data and national security data.

3.2 Data Protection Officer

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

3.3 Data Protection Authority

National authorities tasked with the protection of data and privacy.

3.4 Data Controller

The entity that determines the purposes, conditions and means of the processing of personal data.

3.5 Data Processor

The entity that processes data on behalf of the Data Controller.

3.6 Data Subject

A natural person whose personal data is processed by a controller or processor.

3.7 Personal data

Any information related to a natural person or 'data subject'.

3.8 Processing

Any operation performed on personal data, whether automated or not.

3.9 Recipient

The entity to which personal data is disclosed.

4 The GDPR

4.1 Background

The GDPR is based on the 1980 Protection of Privacy and Transborder Flows of Personal Data Guidelines, which outlined eight principles:

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

4.2 NHS Digital

The Information Governance Alliance (IGA) is the authority that gives advice and guidance on the rules governing the use and sharing of healthcare-related information for the NHS. NHS Digital provides up-to-date information regarding the GDPR as well as a range of useful guidance documentation.

4.3 Aim of the GDPR

The GDPR was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way in which organisations across the region approach data privacy.

4.4 Brexit and the GDPR

Despite leaving the EU, the GDPR will still be enforced, as it applies prior to the UK leaving the EU. The Regulation became applicable as law in the UK as of the 25th May 2018.

4.5 GDPR and DPA 2018

To ensure that organisations have a complete overview of the legislation as of 25th May 2018, it will be necessary to view the GDPR and DPA 2018 side by side.

5 Roles of data controllers and processors

5.1 Data controller

At College Health surgeries the role of the data controller is to ensure that data is processed in accordance with Article 5 of the Regulation. He/she should be able to demonstrate compliance and is responsible for making sure data is:

- 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 College Health Surgeries is either the Practice or Patient Services Manager, these details are displayed in each surgery; they are responsible for ensuring that all data processors comply with this policy and the GDPR.

5.2 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:

- 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 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 controller
- 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

At College Health surgeries all staff are classed as data processors as their individual roles will require them to access and process personal data.

6 Access

6.1 Data subject's rights

All data subjects have a right to access their data and any supplementary information held by College Health. Data subjects have a right to receive:

- Confirmation that their data is being processed
- Access to their personal data
- Access to any other supplementary information held about them

College Health ensures that all patients are aware of their right to access their data and has privacy notices displayed in the following locations:

- Waiting room
- Practice website
- Practice information leaflet

To comply with the GDPR, all practice 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 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 authorize third-party access, e.g. for solicitors and insurers, under the GDPR.

6.2 Fees

Under the GDPR, College Health is not permitted to charge data subjects initial access; this must be done free of charge. In instances where requests for copies of the same information are received or requests are deemed "unfounded, excessive or repetitive", a reasonable fee may be charged. Furthermore, a reasonable fee may be. However, this does not permit the practice to charge for all subsequent access requests.

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

6.3 Responding to a data subject access request

In accordance with the GDPR, data controllers must respond to all data subject access requests within one month of receiving the request (previous subject access requests had a response time of 40 days). It is the guidance of the BMA that a universal aapproach is applied and a 28-day response time implemented.

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.

6.4 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 practice 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.

6.5 E-requests

The GDPR states that data subjects should be able to make access requests via email. College Health is compliant with this and data subjects can complete an e-access form and submit the form via email.

The data controller is to ensure that ID verification is requested and this should be stated in the response to the data subject upon receipt of the access request. It is the responsibility of the data controller to ensure they are satisfied that the person requesting the information is the data subject to whom the data applies.

6.6 Third-party requests

Third-party requests will continue to be received following the introduction of the GDPR. 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 College Health Ltd will request that third parties complete this form.

6.7 Access to Medical Records Policy

Detailed guidance regarding subject access requests can be found in the practice's Accesss to medical Records Policy which can be found on GP Team Net

6.8 Requests from Insurers

The information Commissioners Office (ICO) refers to the use of SARs to obtain medical information for insurance purposes as being in fact an abuse of access rights, and the processing of full medical records by insurance companies risks breaching the GDPR.

Therefore, College Health Ltd will contact the patient to explain the extent of the disclosure sought by the third party. The practice can then provide the patient with the medical records as opposed to the insurer. The patient is then given the opportunity to review their

record and decide whether they are content to share the information with the insurance company.

College Health will advise insurers to use the Access to Medical Reports Act 1988 when requesting a GP report. The following fees are applicable:

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

7 Data breaches

7.1 Data breach definition

A data breach is defined as any incident that has affected the confidentiality, integrity or availability of personal data. Examples of data breaches include:

- Unauthorised third-party access to data
- Loss of personal data
- Amending personal data without data subject authorisation
- The loss or theft of IT equipment which contains personal data
- Personal data being sent to the incorrect recipient

7.2 Reporting a data breach

Any breach that is likely to have an adverse effect on an individual's rights or freedoms must be reported. In order to determine the requirement to inform the ICO, to notify them of a breach, the data controller is to read ICO – Personal Data Breaches, this document is available on GP teamnet. Breaches must be reported without undue delay or within 72 hours of the breach being identified.

When a breach is identified and it is necessary to report the breach, the report is to contain the following information:

- Organisation details
- Details of the data protection breach
- What personal data has been placed at risk
- Actions taken to contain the breach and recover the data
- What training and guidance has been provided
- Any previous contact with the Information Commissioner's Office (ICO)
- Miscellaneous support information

The ICO data protection breach notification form (available on GP teamnet) should be used to report a breach. Failure to report a breach can result in a fine of up to €10 million.

The data controller is to ensure that all breaches at their surgery are recorded; this includes:

- Documenting the circumstances surrounding the breach

- The cause of the breach; was it human or a system error?
- Identifying how future incidences can be prevented, such as training sessions or process improvements

7.3 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 that surgery 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

8 Data erasure

8.1 Erasure

Data erasure is also known as the "right to be forgotten", which enables a data subject to request the deletion of personal data where there is no compelling reason to retain or continue to process this information. It should be noted that the right to be forgotten does not provide an absolute right to be forgotten; a data subject has a right to have data erased in certain situations.

The following are examples of specific circumstances for data erasure:

- Where the data is no longer needed for the original purpose for which it was collected
- In instances where the data subject withdraws consent
- If data subjects object to the information being processed and there is no legitimate need to continue processing it
- In cases of unlawful processing
- The need to erase data to comply with legal requirements

The data controller can refuse to comply with a request for erasure in order to:

- Exercise the right for freedom of information or freedom of expression
- For public health purposes in the interest of the wider public
- To comply with legal obligations or in the defence of legal claims

8.2 Notifying third parties about data erasure requests

Where a College Health surgery 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; this is so long as it is achievable and reasonably practical to do so.

This policy will be updated once the NHS IGA have issued guidance regarding data erasure.

9 Consent

9.1 Appropriateness

Generally, consent will not be the ground that your practice will be relying on for the provision of primary care.

However, if your practice operates a newsletter or other method of updating patients on what 's going on at the practice then consent will be needed.

Such communication count as marketing and the non-consent based grounds that apply to the provision of primary care will not apply here.

GDPR set a new higher standard for consent, as it must be 'freely given, specific and informed'.

This means that where consent is being relied on it requires a positive opt in. You cannot use pre-ticked boxes or negative opt-out statements e.g. Tick the box if you do not wish to receive new and updates from us.

9.2 Obtaining consent

If it is deemed appropriate to obtain consent, the following must be explained to the data subject:

- Why the practice wants the data
- How the data will be used by the practice
- The names of any third-party 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 each College Health surgery it is the responsibility of the data controller 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.

An email/text consent form is available on GP teamnet under GDPR Documents.

9.3 Parental consent

Whilst the GDPR states that parental consent is required for a child under the age of 16, the DPA 2018 will reduce this age to 13 in the UK. Additionally, the principle of Gillick competence remains unaffected; nor is parental consent necessary when a child is receiving counselling or preventative care.

10 Data mapping and Data Protection Impact Assessments

10.1 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 all College Health employees 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.

Annex A details the process of data mapping at College Health Ltd.

10.2 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 College Health Ltd will be involved in the mapping process, thus enabling the wider gathering of accurate information.

10.3 Data Protection Impact Assessment

The DPIA is the most efficient way for College Health Ltd 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 GDPR, 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; then 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 process, including the purpose
- 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 College Health Ltd 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.

10.4 DPIA process

The DPIA process is formed of the following key stages:

- Determining the need
- Assessing the risks associated with the process
- Identifying potential risks and feasible options to reduce the risk(s)
- Recording the DPIA
- Maintaining compliance and undertaking regular reviews

Annex B provides a template that is to be used to carry out a DPIA at each College Health surgery.

11 Summary

Given the complexity of the GDPR, all staff at College Health Ltd must ensure they fully understand the requirements within the Regulation. Understanding the changes required will ensure that personal data at College Health Ltd remains protected and the processes associated with this data are effective and correct.

Regular updates to this policy will be applied when further information and/or direction is received.

Annex A – The data mapping process

WHY is personal data processed?	
Personal data is defined as any information relating to a natural person or "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 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. • CCTV • Use of IT • Minutes of meetings	• Contact details • Health records • NOK details • Referrals • Prescriptions • CCTV • Online service/practice apps • PPG membership, minutes etc.
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 • Cleaners • Pharmacy • Equipment servicing/repair	• Reps • Guest speakers • Trainers
List whose personal data is processed:	

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 licence etc.)	**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.)
Sharing and disclosure	**Sharing and disclosure**
• Appraisal • References • Awards and recommendations • OH • Incident reports / forms • Business cases • Insurance and banking	• Referrals • Results • Letters to other service providers
Retention	**Retention**
• For 7 years after the staff member has left College Health's employment	• For 3 years after the death of the patient

List when personal data is processed:		
Obtained / updated	**Disclosure (with who & 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	• 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 & 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)	Electronic records – SystmOne Manual record – Lloyd George wallet – Administration office

Annex B – The Data Protection Impact Assessment

This document is to be used to conduct a DPIA at [insert practice name].

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 which 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 which 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?	
Information use – Is the data obtained for specified, explicit and legitimate purposes?	
What is the purpose for 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?	
Information attributes – Personal data shall be accurate and, where necessary, kept up to date	
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?	
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?	
What controls are in place to safeguard only authorised access to the data?	

How is data transferred; is the process safe and effective?	
Data subject access – Personal data shall be accurate and, where necessary, kept up to date	
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?	
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?	
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?	
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?	
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?	

Continued overleaf...

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 practice'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. This can be amended on a practice to practice basis.

Step 5 – Reviewing the DPIA

The review process is detailed in the report.

Data Protection Impact Assessment Report	
Practice name	**[Insert practice name]**
Data controller	**[Insert name of controller]**
Date of assessment	**[Insert date]**
Process assessed	**[Referral process]**

Overview:

[Insert practice 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 GPDR, which comes into effect on 25th May 2018, 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 practice is frequently required to share data subjects' personal data – more specifically, personal details and healthcare between organisations. That is the sharing of data between College Health practices and Basildon and Thurrock Hospitals NHS Trust in Thurrock. 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 Systmone Web clinical system
Is the use of the information linked to the reason(s) for the information being collected?	Yes

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	Yes, authority must be provided by the third party who also included either a written

unauthorised access?	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]

Annex C – GDPR checklist

This checklist has been designed to support practice managers in preparing for the GDPR.

Creating a culture of awareness	
All staff need to be aware that the GDPR becomes applicable by law in the UK as of the 25th May 2018. • It is essential that they understand the impact this will have on them in their roles. • Have you shared the practice GDPR policy with them or signposted them to further information, i.e. ico.org.uk or NHS Digital IGA?	
Action complete (✓ or ✗)	

Understanding the information flow	
The practice must understand why, whose, what, when and where personal data is processed. • Conducting a data-mapping exercise will enable practices to do this. • Data-mapping is not a one-person task; all staff should be involved, enabling the wider gathering of accurate information.	
Action complete (✓ or ✗)	

Data Protection Impact Assessment (DPIA)	
The DPIA is the most efficient way for the practice to meet their data protection obligations. DPIAs are mandatory in accordance with Article 35 of the GDPR and should be undertaken when: • 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 which present similar high risks • Extensive processing activities are undertaken, including large-scale processing of personal and/or special data Have DPIAs been completed? Best practice is to undertake DPIAs for existing processes to ensure that data protection obligations are met.	
Action complete (✓ or ✗)	

Continued overleaf…

Updating privacy information	
All data subjects must understand how their data will be used. • Have you updated your practice privacy notice and are all staff aware of the changes? • Have you displayed the privacy notice in prominent positions such as the waiting room, consulting rooms, website, and updated the practice information leaflet? • Is your privacy notice in a language that is understandable to all patients? • Does it comply with Articles 12, 13 and 14 of the GDPR?	
Action complete (✓ or ✘)	

The rights of the data subject	
All data subjects have rights. Has this been communicated or is information displayed to reflect this, and does it include the: • Right of access • Right to erasure (or right to be forgotten) • Right to data portability • Right to object • Right to rectification • Right to restriction of processing • Right to notification • Right not to be subject to automated decision-making (including profiling)	
Action complete (✓ or ✘)	

Subject access requests	
All data subjects have a right to access their data and any supplementary information held. Does the practice policy reflect the changes and do staff understand: • The changes affecting subject access requests? • There is no fee applicable as of 25th May 18? • The response time is one calendar month? • Requests can be refused, but must be fully justified? • Requests can be received by email?	
Action complete (✓ or ✘)	

Processing personal data
Do data processors within the practice understand that they are responsible for the processing of data on behalf of the data controller? Do all processors know that one of the following must apply: • 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 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 controller

• 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
Action complete (✓ or ✗)

Consent
Consent is an area that has seen significant change as a result of the GDPR. • Do current processes for obtaining consent reflect the GDPR? • Do staff know that they must explain to data subjects: Why the practice wants the data How the data will be used by the practice The names of any third-party controllers with whom the data will be shared Their right to withdraw consent at any time • Are staff aware that the Data Protection Bill (DPA 2018) will state that parental consent is required for a child under the age of 13; Gillick competence remains unaffected
Action complete (✓ or ✗)

Data breaches
What are the current procedures to detect and report data breaches? • Do staff know what a data breach is? • What is the reporting process? • Is there a process to notify data subjects of a breach affecting them? • How are data breaches recorded; who is responsible for this? • Does the practice policy include data breaches and responsibilities?
Action complete (✓ or ✗)