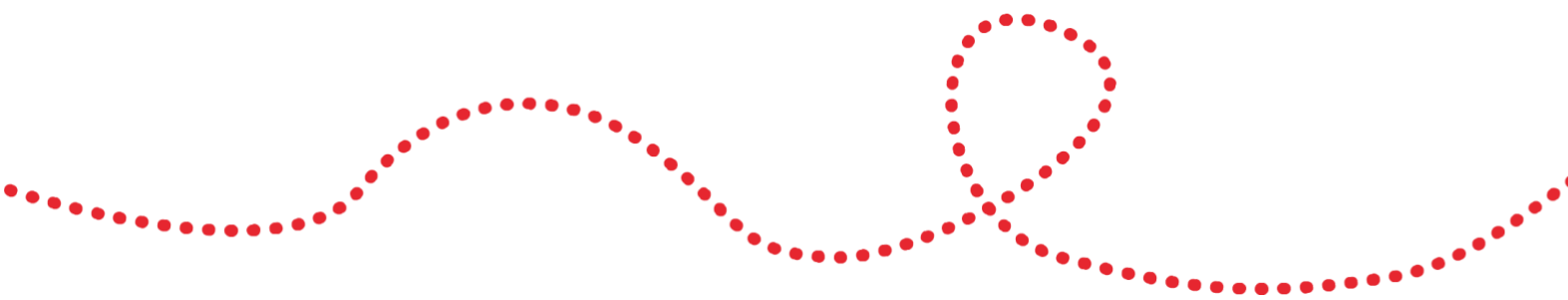
Heartbeat
Connecting health and care communities

GDPR COMBINED POLICIES AND PROCEDURES

Version	1
Date	09.12.2021
Approval date	18 April 2018
Approved by	Lisa Pammen
Author	Lynn Irwin
RENEWAL DATE	April 2021 – done December 2024



General Data Protection Regulation Policy

And Related Practice Policies

Table of contents

1 Introduction 5
1.1 Policy statement 5
1.2 Training and support 5

2 Scope 5
2.1 Who it applies to 5
2.2 Why and how it applies to them 5

3 Definition of terms 6
3.1 Data Protection Officer 6
3.2 Data Protection Authority 6
3.3 Data Controller 6
3.4 Data Processor 6
3.5 Data Subject 6
3.6 Personal data 6
3.7 Processing 6
3.8 Recipient 6

4 The build-up to the GDPR 7
4.1 Background 7
4.2 NHS Digital 7
4.3 Aim of the GDPR 7
4.4 Brexit and the GDPR 7

5 Roles of data controllers and processors 8
5.1 Data controller 8
5.2 Data processor 8

6 Access 9
6.1 Data subject's rights 9
6.2 Fees 9
6.3 Responding to a data subject access request 9
6.4 Verifying the subject access request 10
6.5 E-requests 10
6.6 Third-party requests 10

7 Data breaches 9
7.1 Data breach definition 9
7.2 Reporting a data breach 9
7.3 Notifying a data subject of a breach 12

8 Data erasure 11
8.1 Erasure 11
8.2 Notifying third parties about data erasure requests 11

9 Consent 12
9.1 Appropriateness 12
9.2 Obtaining consent 12

10 Preparing for the GDPR 13
10.1 Data mapping 13
10.2 Data mapping and the Data Protection Impact Assessment 13
10.3 Data Protection Impact Assessment 13
10.4 DPIA process 13

11 Summary 14

RELATED POLICIES:

Access to Health Records Application 15
Computer and Data Security 17
Computer, Internet and E-Mail Usage 25
Correspondence, Reports and Results 31
Data Protection 34
Information Governance 36
Processing Personal Data Held on Staff - Staff Information and Consent Form 40
Records Retention 45
Smartcard Usage Declaration 50

Annex A – The data mapping process 52

Annex B – The Data Protection Impact Assessment 57

1 Introduction

1.1 Policy statement

The EU General Data Protection Regulation (GDPR herein) will come into force on 25th May 2018, superseding the Data Protection Act (DPA) 1998. The GDPR applies to all EU member states and Central Dales Practice must be able to demonstrate compliance at all times. Understanding the requirements of the GDPR will ensure that personal data of both staff and patients is protected accordingly.

1.2 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

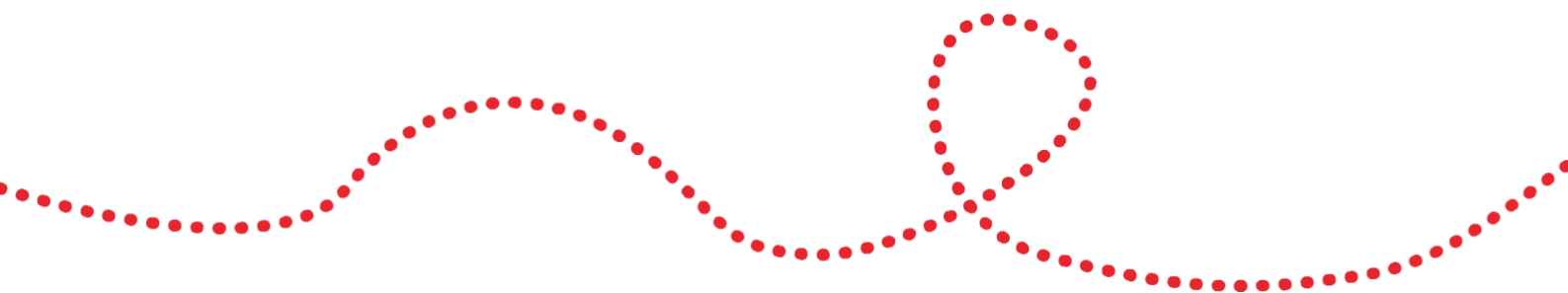
2.1 Who it applies to

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

All personnel at Central Dales Practice 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 Officer

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

3.2 Data Protection Authority

National authorities tasked with the protection of data and privacy.

3.3 Data Controller

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

3.4 Data Processor

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

3.5 Data Subject

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

3.6 Personal data

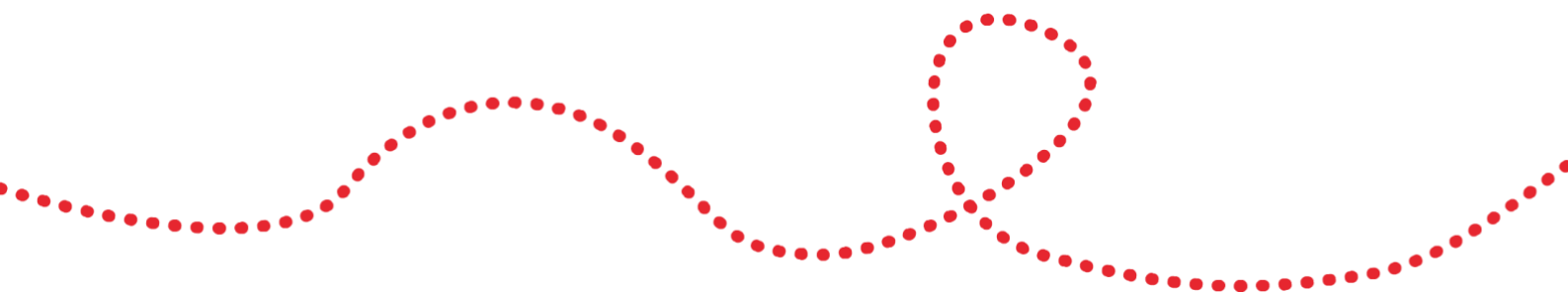
Any information related to a natural person or ‘data subject’.

3.7 Processing

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

3.8 Recipient

The entity to which personal data is disclosed.



4 The build-up to 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. As a result of the imminent introduction of the GDPR, an NHS policy is being developed by the GDPR working group and will be published in due course.

NHS Digital provides up-to-date information regarding the GDPR as well as a range of useful guidance documentation.[1]

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.[2]

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 will be applicable as law in the UK with effect from 25th May 2018.

[1] NHS Digital GDPR guidance
[2] EU GDPR overview

5 Roles of data controllers and processors

5.1 Data controller

At Central Dales Practice 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:[3]

- 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 Central Dales Practice is Caroline Garrard, Practice Manager; 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:[4]

- 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

[3] Article 5 GDPR Principles relating to processing of personal data

[4] Article 6 Lawfulness of processing

- 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 Central Dales Practice, 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 Central Dales Practice. 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

The purpose for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them.

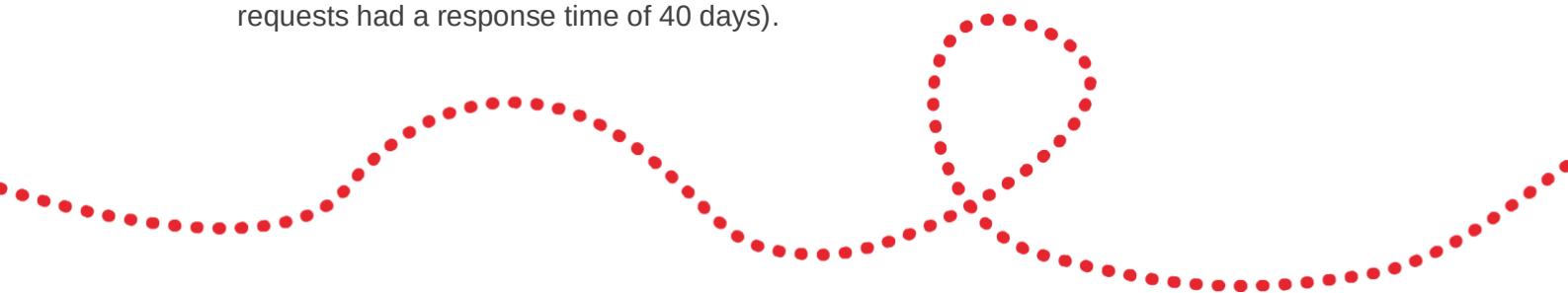
6.2 Fees

Under the GDPR, Central Dales Practice is not permitted to charge data subjects for providing a copy of the requested information; this must be done free of charge. That said, should a request be deemed either "unfounded, excessive or repetitive", a reasonable fee may be charged. Furthermore, a reasonable fee may be charged when requests for additional copies of the same information are made. 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).



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 license or passport.

6.5 E-requests

The GDPR states that data subjects should be able to make access requests via email. Central Dales Practice is compliant with this and data subjects can complete the SAR form and submit via email or the practice website.

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.

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.[5] 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 this supporting guidance.

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 should be used to report a breach. Failure to report a breach can result in a fine of up to €10 million.[6]

The data controller is to ensure that all breaches at Central Dales Practice are recorded; this includes:

[5] ICO – Personal data breaches
[6] ICO Personal data breaches

- 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 Central Dales Practice 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 Central Dales Practice 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

Consent is appropriate if data processors are in a position to "offer people real choice and control over how their data is used".[7] The 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.

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

Although the NHS IGA have not issued definitive guidance on this subject, it is anticipated that consent will be detailed in depth in the NHS GDPR advice material. This policy will be updated to reflect the NHS guidance when published.

[7] ICO Consent

10 Preparing for the GDPR

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 Central Dales Practice 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 Central Dales Practice.

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 Central Dales Practice 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 Central Dales Practice 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

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:

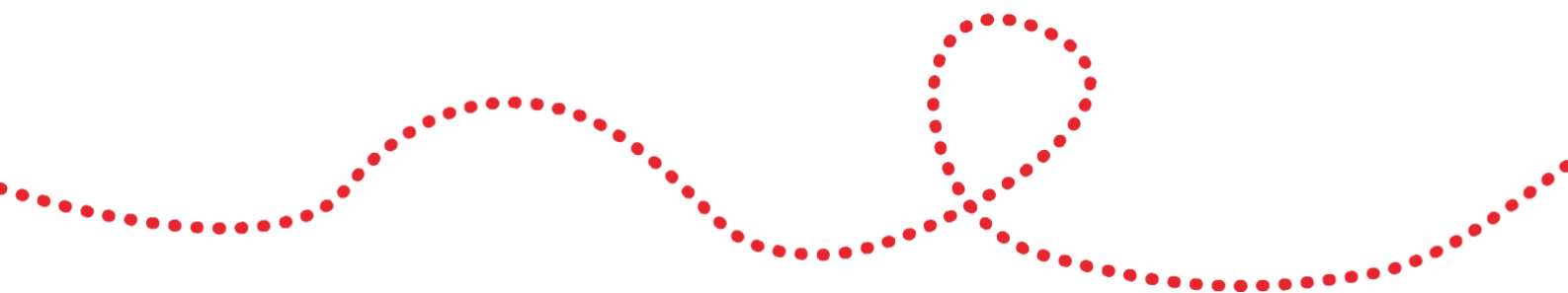
- Determining the need
- Assessing the risks associated with the process
- Identifying potential risks and feasible options to reduce the risk(s)
- Recording the DPIA
- Maintaining compliance and undertaking regular reviews

Annex B provides a template that is to be used to carry out a DPIA at Central Dales Practice.

11 Summary

Given the complexity of the GDPR, all staff at Central Dales Practice must ensure they fully understand the requirements within the Regulation, which become enforceable by law with effect from 25th May 2018. Understanding the changes required will ensure that personal data at Central Dales Practice 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.



APPLICATION FOR ACCESS TO MEDICAL RECORDS
Data Protection Act 1998 Subject Access Request

Details of the Record to be accessed:

Patient Surname	NHS Number
Forename(s)	Address
Date of Birth	

Details of the Person who wishes to access the records, if different to above:

Surname	
Forename(s)	
Address	
Telephone Number	
Relationship to Patient	

Declaration: I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health records referred to above under the terms of the Data Protection Act 1998.

Tick which ever of the following statements apply.

- ☐ I am the patient.
- ☐ I have been asked to act by the patient and attach the patient's written authorisation.
- ☐ I am acting in Loco Parentis and the patient is under age sixteen, and is incapable of understanding the request / has consented to me making this request.
  (*delete as appropriate).

☐ I am the deceased patient's Personal Representative and attach confirmation of my appointment.

☐ I have a claim arising from the patient's death and wish to access information relevant to my claim on the grounds that….(please supply your reasons below).

Your Signature .....Date.....

Note: **There is a fee of £10 for access to records. An additional fee of 24p per page is charged if records are to be photocopied up to a maximum of £50. The fee must accompany this request. Cheques to be payable to Central Dales Practice, 21 days prior notice is usually required.**

Details of my Application

Patient to complete (please tick as appropriate)

I am applying for access to view my records only	
I am applying for copies of my medical record	
I have instructed someone else to apply on my behalf	
I have attached the appropriate fee	

Notes:

Under the Data Protection Act 1998 you do not have to give a reason for applying for access to your health records.

Optional - Please use this space below to inform us of certain periods and parts of your health record you may require, or provide more information as requested above.

This may include specific dates, consultant name and location, and parts of the records you require e.g. written diagnosis and reports. Note: defining the specific records you need may result in lower fee charges and a quicker response.

I would like a copy of all records	

I would like a copy of records between specific dates only (please give date range) below	
I would like copy records relating to a specific condition / specific incident only (please detail below)	

COMPUTER AND DATA SECURITY PROCEDURE

(Incorporating Request to Work From Home)

INTRODUCTION

The purpose of this procedure is to define the arrangements and responsibilities for the physical security of computer hardware, backup of computer data, verification that the backups are effective, storage of backup data, and also to set out the basis on which software additions may be made to individual PCs, the system or the network.

It is essential that the Practice has full and accessible data backups so that in the event of any system failure data can be restored so that normal operations can be resumed quickly and effectively.

There are also a number of precautions to be taken to protect the physical security of computers. These precautions depend on the situation. Different precautions need to be taken for computers used away from the workplace and for laptops used in a variety of locations.

The clinical system used is SystmOneWeb and all patient medical records and information are stored and backed up off site in a central location.

As part of our contingency planning, the appointment book is backed up daily to a memory stick and kept in the safe.

In view of the accidental releases of personal data from a variety of government organisations, it is generally recognised that the risk involved in transporting data “off site” is far greater than the risk of accidental destruction or loss whilst the information is on the prSystmOnees, and the Chief Executive of the NHS wrote to Primary Care Organisations in December 2007 to ensure that:

- Patient identifiable information is secure
- Data transfer methods are secure
- That remedial action is being taken if these two issues are weak

In addition:

- Personal identifiable information is not to be stored on removable devices such as CDs, memory-sticks. Floppy discs, external hard-drives etc unless it is encrypted
- Data is not to be downloaded or stored on portable media such as laptops, mobile phones, PDAs etc unless it is encrypted
- Personal identifiable information is not to be stored on PC equipment in non-secure areas unless it is encrypted.
- All video camera equipment and tapes with video consultations are to be stored in the safe until destruction is arranged.

And these requirements apply to all public sector organisations.

Given the complexity of adequate encryption tools the above requirements will be enforced within the Practice pending further instructions.

Storage and Backup

Any data stored on a computer hard drive is vulnerable to the following:

- Loss due to a computer virus.
- Physical loss or damage of the computer, for example:
    - Theft
    - Water damage
    - Fire or physical destruction
    - Faulty components
    - Software

In particular, there is a risk of breach of confidentiality where a computer is stolen or otherwise falls into unauthorised hands.

The following precautions should be taken:

- Servers should not be used as regular workstations for any application
- Access to servers will be authorised
- Use a shared drive on a networked server for all data wherever possible
- Backups will be stored in a fireproofed safe ie the appointment book.
- No patient data will be stored on a PC or other equipment in non-secure areas
- Take extra precautions to protect the server. Servers should be sited away from risk of accidental knocking, spillage of drinks, leaking pipes, overheating due to radiators and be inaccessible to the public – it is located in the computer room.
- Where a PC is standalone, ensure that the hard drive is backed up regularly and any confidential data is password protected

Four backup tapes are available and should be used in rotation and should be renewed when required. The reception team are responsible for completing the backups each day.

BULK DATA EXTRACTIONS

No bulk extracts or manipulation of data or coding is permitted other than with the prior permission of the Practice Manager.

PROTECTION AGAINST VIRUSES

Data is vulnerable to loss or corruption caused by viruses. Viruses may be introduced from floppy discs, CDROM/DVDROM, other storage media and by direct links via e-mail and web browsing.

The following precautions will be taken:

- Virus protection software will be installed on ALL computer equipment
- Automatic or pre-programmed updates will be used wherever possible
- A clear procedure via nominated staff will deal with any viruses found
- Software installation will be in accordance with this protocol and only authorised licensed software is to be installed on the organisation's equipment
- The Computer, Internet and Email Policy will contain specific instructions on downloads, attachments and unknown senders etc.
- Physical restrictions e.g. drive locks / disable drives will be used where appropriate
- All staff will be made aware of data security issues in all IT related protocols and procedures

INSTALLATION OF SOFTWARE

Software purchases will be authorised by the Practice Manager who will supervise the loading of the software onto the system or individual PCs in accordance with the software licence.

Staff are prohibited from installing or upgrading personal or purchased software without the written permission of the nominated person.

Staff are prohibited from downloading software, upgrades or add-ins from the internet without the written permission of the nominated person.

Staff are permitted to receive and open files received in the normal course of business providing they have been received and virus scanned through the standard virus software installed by the clinical system supplier.

HARDWARE

Staff and contractors are not permitted to introduce or otherwise use any hardware or removable storage devices into the Practice other than that which has been provided, or pre-approved, by the Practice.

The Practice Manager is responsible for ensuring that the Practice has adequate supplies of removable storage media of a type approved for use in the Practice. The use of removable storage media is by authorised staff only.

Removable storage media (including CDs and other similar temporary items) which are no longer required must be stored securely for destruction along with other PC equipment. The Practice Manager will be responsible for the secure storage of these items.

PROTECTION AGAINST PHYSICAL HAZARDS

Water

- Check that the PC or server are not at risk of pipes and radiators which, if damaged, could allow water onto the equipment
- Do not place PCs near to taps/ sinks
- Do not place PCs close to windows subject to condensation and water collection on windowsills
- Ensure that the PC is not kept in a damp or steamy environment

Fire and Heat

- Computers generate quite a bit of heat and should be used in a well-ventilated environment. Overheating can cause malfunction, as well as creating a fire hazard
- Try to place the PC away from direct sunlight and as far as possible from radiators or other sources of heat
- Normal health and safety protection of the building against fire, such as smoke alarms and CO_2 fire extinguishers should be sufficient for computers. If backup tapes are kept on the prSystmOnees they must be protected against fire in a fireproof safe
- Have the wiring and plugs checked annually
- Ensure that ventilators on computers are kept clear
- Do not stack paper on or near computers

Environmental Hazards

Computers are vulnerable to malfunction due to poor air quality, dust, smoke, humidity and grease. A normal working environment should not affect safe running of the computer, but if any of the above are present consider having an air filter. Ensure that the environment is generally clean and free from dust.

Power Supply
Protect against power surges by having an uninterrupted power supply fitted to the server.

In the event of the prSystmOnees becoming unusable, a pre-tested 'IT Disaster Recovery Procedure' needs to ensure that systems can be run off site, including replacement hardware.

Protection against Theft or Vandalism via Access to the Building

In addition, the following precautions should be considered to protect the building, such as:

- Burglar alarm with intruder monitor in various locations
- Locks on all downstairs windows
- Appropriate locks or keypad access only, on all doors
- Seal off separate areas of the building e.g. reception area should have shutters and a lockable door, and all separate rooms should be locked when the building is unoccupied
- Where the building is not fully occupied e.g. during out of hours clinics, only the required rooms and corridors should be accessible to the public e.g. admin areas and consulting rooms not in use to be kept locked
- Ensure there is a clear responsibility for locking the doors and securing the building when unoccupied
- Ensure any keys stored on site are not in an obvious place and any instructions regarding key locations or keypad codes are not easily accessible
- Have a procedure for dealing with unauthorised access during opening hours
- Ensure that there is appropriate insurance cover where applicable
- Do not store patient identifiable information on PC equipment which is not contained in a secure area
- Maintain a separate record of hardware and software specifications of every PC in the building
- Specific precautions relating to IT hardware are:
    - Use security locks to fix IT hardware to desks to prevent easy removal
    - Locate PCs as far away from windows as possible
    - Clearly 'security mark' all PCs and all parts of PCs i.e. screen, monitor, keypad.
    - Have an asset register for all computer equipment, which includes serial numbers
    - Ensure every PC is password protected

MOBILE COMPUTING

Particular precautions need to be taken with portable devices, both when they are used on site and when taken offsite.

On-site

Laptops, palmtops and any other portable devices are more vulnerable than PCs, because they are easier to pick up and remove and therefore more desirable to the opportunist thief. It is also less likely, in some circumstances, that their loss will be noticed immediately. However, because of their size, it is possible to provide extra protection:

- When the device is not in use, it should be stored in a secure location
- Where it is left on the prSystmOnees overnight, it should be stored in a locked cupboard or drawer
- Where the device is shared, have a mechanism for recording who is responsible for it at any particular time
- Patient or personal identifiable information should not be contained on laptops or other portable devices or removable storage devices

In transit

Computers should not be left unattended in cars. Where this is unavoidable, ensure that the car is locked and the computer is out of site in the boot or at least covered up if there isn't a boot.

The responsible staff member should take the device with them if leaving the vehicle for any length of time.

Use in a Public Place

- The device should remain with the member of staff at all times
- Care should be taken when using the device that confidential data cannot be overlooked by members of the public e.g. on public transport

Use in a Patient's Home

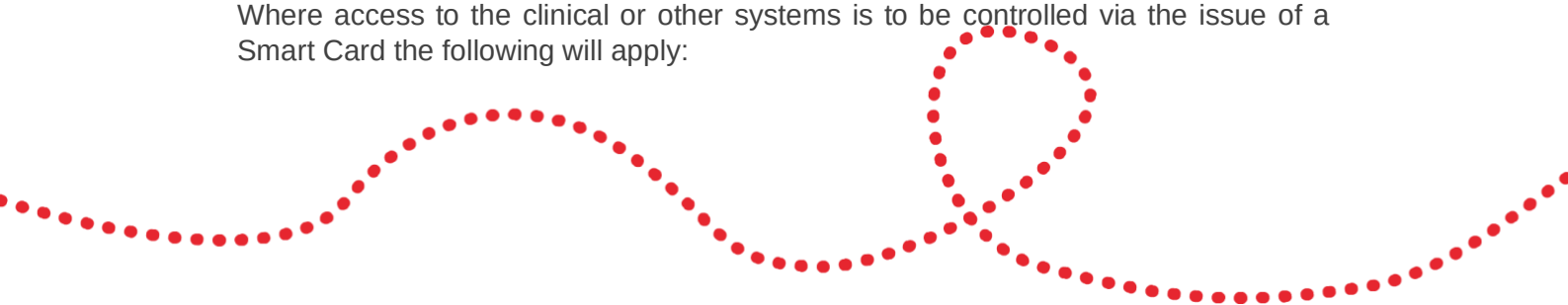
- The device should have a password protected screen saver
- The device should remain with the member of staff at all times
- Care should be taken that confidential data cannot be seen by other members of the family / carers

Use on other prSystmOnees (e.g. outreach clinic)

- The device should remain with the member of staff at all times
- When the device is not in use it should be stored in a secure location
- Where it is left on the prSystmOnees overnight, it should be stored in a locked cupboard or drawer

SMART CARDS

Where access to the clinical or other systems is to be controlled via the issue of a Smart Card the following will apply:



- Smart cards are issued to an individual on a named basis and are for the use of that person only
- The access level relating to an individual is personal and must not be shared or otherwise made accessible to another member of staff
- The Smart Card is to be kept under the personal control of the individual to whom it has been issued at all times and must not be left inserted into a smart card reader when the individual is not present
- The Smart Card will normally be held on a neck cord or other similar device to ensure that it remains with the owner
- On leaving a terminal the Smart Card is to be removed ***on every occasion***
- Staff members are not to leave their cards on the prSystmOnees when they leave work, unless they are locked in the control drug cupboard
- Staff members leaving their cards at home will be required to go and collect it
- Staff members sharing Smart Cards on more than one occasion will be considered for disciplinary action in accordance with the Practice's normal procedures. This would normally be after an informal warning
- Staff members must report the loss of a card to the Practice Manager as soon as it is known that the card is missing
- Smart Cards will not normally be handed over between individuals. In the event of a staff member needing to relinquish a card (e.g. over a holiday period) then this will be passed back to the Practice Manager or nominated person who will log the transfer and retain the card securely

HOME WORKING

In some instances it may be appropriate for a member of staff to work at home. Careful consideration needs to be given to the following issues:

- Will the member of staff be using their employers PC or their own?
- Will the member of staff have dial in access to the organisation's systems?
- Will the member of staff be using the organisation's confidential data for work purposes or for the individual's own purposes (coursework, research etc)?
- Does the staff member require separate registration under the Data Protection Act?

Under no circumstances will patient or personal identifiable information be permitted to be removed from the prSystmOnees in any format without the express permission of the Data Controller. Work at home is anticipated to relate to administration or non-personal information only.

Employee's own PC without dial in access

The following should be considered:

- Physical security of the PC – vulnerability to theft or unauthorised access

- Unauthorised access to confidential data by other family members using the computer
- Risk of loss of the data due to viruses, accidental loss etc.
- Back-up of essential data
- Disposal of printouts of confidential data generated at the employee's home
- Ensuring the data is fully deleted from the computer after use
- Ensuring the employee does not use the data for any purpose other than for that authorised
- If the work is on going, ensuring that the data is destroyed when the employee leaves employment or replaces their home computer

Employee's own PC with dial in access

The following should be considered:

- Ensure that strong authentication is in place
- Ensure that data is not held on the computer hard drive
- Ensure that other modems are not attached to the computer, as this invalidates the organisations "code of connection" and places the systems security at risk
- Disposal of printouts of confidential data generated at the employee's home

Using an NHS Organisation's Computer

- Physical security of the computer
- Unauthorised access to confidential data by other family members using the computer
- Ensure that strong authentication is in place
- Ensure that up to date virus protection is in place
- Ensure that other modems are not attached to the computer, as this invalidates the organisation's "code of connection" and places the system at risk
- Disposal of printouts of confidential data generated at the employees' home
- Ensuring the employee does not use the data for any purpose other than that authorised for
- Ensure that no data is held on the computer hard drive where the employee has dial in access

The Practice's Responsibilities

The Practice must ensure that the employee fully understands all their responsibilities with regard to confidential data. The employee must sign a written statement of the responsibilities they are undertaking towards the security of the data.

The Practice must ensure that there are arrangements to clear employees' hard drives of any confidential data as soon as this becomes appropriate.

The Practice must ensure that arrangements are in place for the confidential disposal of any paper waste generated at the employees' home.

The Practice must maintain an up-to-date record of any data being processed / accessed at an employee's home, and the purpose for which the employee is accessing the data. It is the employee's responsibility to use the data for the purpose intended and no other, and they must be absolutely clear as to what that purpose is.

The Practice must be clear as to when it is passing ownership of data to an individual (e.g. for project work or, research and development) and this should be authorised by the Caldicott Guardian / Data Controller. The individual may then need to be separately registered under the Data Protection Act 1998.

Computer, Internet and E-Mail Usage Protocol

INTRODUCTION

- The practice's computers and IT network are invaluable resources which must be used appropriately.
- The internet offers access to almost infinite sources of information
- E-mail offers a fast, inexpensive and convenient way to communicate both inside and outside the practice.
- The practice wishes to ensure that these resources are used responsibility and productively

APPLICABILITY

The policy applies to all employees and to other people who work at the Practice, e.g. locum GP's, non-employed nursing staff, temporary staff and contractors who have access to the practice's computer systems.

THE POLICY

Clinical Computer System (SYSTMONE) and Desk Top Computer System

- All information about patients is confidential: from the most sensitive diagnosis, to the fact of having visited the surgery or being registered at the Practice.

- All patients can expect that their personal information will not be disclosed without their permission (except in the most exceptional circumstances when disclosure is required when someone is at grave risk of serious harm).

- **Viewing of patients medical records (either electronic or paper) should only be carried out on a need to know basis.**

- Clinical data must not be taken from the Practice's computer system (e.g. on a memory stick or removable drive) off the prSystmOnees unless authorised to do so by the Practice Manager.

- Any breach of confidentiality will be considered as a serious disciplinary offence and may lead to dismissal.

- You remain bound by the requirement to keep information confidential even if you are no longer employed by the Practice. Any breach, or suspected breach, of confidentiality after leaving the Practice's employment will be passed to the Practice's solicitors for action.

- You must log out of the system and switch off your computer at the end of your working day.

- A weekly back up of any material stored on your computer hard drive is recommended, however we would encourage you to store all data in your personal folder on the shared server (if set up).

User ID / password

- You must use your ID and password to access the computer network.

- You must keep your passwords secret and never disclose them to anyone.

- You must not store your user ID and password or authentication device near your computer.

- Your user ID/password is for your exclusive use. You must not share it or lend it to anyone else.

- If you are signed on to a PC and you are going to leave it unattended for any time, you must activate a lock (Ctrl-alt-Delete) and use the lock option

- If you are signed on to SystmOne and you are going to leave the screen unattended for any time, you must remove your smartcard which automatically logs you out of SYSTMONE and take the card with you.

Virus protection

- For protection, the latest anti-virus software will be installed onto the computer network. You must not remove this software yourself.

- If the anti-virus software detects a possible virus, an on-screen warning message will be displayed. If you see this message you must report it to the Practice Manager or IT Administrator immediately. Do not attempt to remove the virus and do not panic!

- If the anti-virus software detects a possible virus and you can not report it immediately to the Practice Manager or IT Administrator, turn off the PC and **do not use it again until the problem has been investigated by the Practice Manager or IT Administrator.**

- If you suspect that a virus has bypassed the anti-virus software on your PC, report it immediately to the Practice Manager or IT Administrator. **Do not use the PC again until the Practice Manager/IT Administrator gives you the go ahead.**

- You must virus check any files created outside the surgery's control, particularly files/data from the internet, before you load and open them onto your PC.
- No software should be installed onto the computer without approval from the Practice Manager.

E-Mail

- E-Mail messages (internal and external) should be treated with the same care as traditional written communications. Any messages sent to other NHS Agencies etc. could be seen to represent the views and opinions of the whole practice.

- All messages must be written on a professional manner with appropriate language and content. In particular, they must not contain any personal, untrue or defamatory statements about any individual within the surgery which will be considered to be an act of bullying/harassment.

- Because the Internet and e-mail transmissions are not always secure, you must not use them to send confidential or 'surgery' sensitive information to anyone other than those verified by the Practice Manager. If you are in doubt as to whether information is confidential or not, please seek guidance from the Practice Manager. Any patient sensitive information can only be emailed from a .net account to a .net account.

- If you receive an e-mail message that contains material that it inappropriate you must report it immediately to the Practice Manager or IT Administrator. Under no circumstances should such mail be forwarded to another individual or stored on surgery computers. Inappropriate material includes words or pictures that could be considered obscene, offensive, defamatory or illegal, chain mail, hate speech, pornography and messages which are inconsistent with government legislation, i.e. equal opportunity, race and harassment policies. This list is illustrative, BUT NOT EXHAUSTIVE.

- All e-mails are liable to be intercepted. Where inappropriate messages originate from within the surgery, disciplinary action will be taken.

- Where an intercepted e-mail is attempting to come into our system, then we will endeavour to identify the sender. Where the e-mail has come from another surgery/company, the surgery/company will be informed of the identity of the individual and the nature of the e-mail.

- The dissemination of inappropriate material is strictly forbidden. It may result in dismissal and may also constitute a criminal offence.

- If you receive an offensive message, you must report the incident to the Practice Manager.

- In cases of obscene and offensive e-mails, the information will be passed onto the Police for possible prosecution.

GUIDELINES FOR THE USE OF EMAIL

Email communication should be efficient (quick, accurate and convenient) but if used without a simple structured approach it can be just the opposite. When using email for non-social communication there are some basic but important considerations:

1. Is it just a short statement/enquiry or is it a more substantial message/report?
   - Brief messages, questions or responses are ideal for emailing.

- With longer document it may be better to send as an attachment that can be easily saved/filed by recipients. Attached documents should be sent RTF format ("*.rtf" as opposed to "*.doc") as this is much less likely to allow viruses to be carried and it can be read by different applications.

2. What is the priority?

- Routine information can be readily sent by courier/post which will help avoid over-use of email which can detract from its usefulness.
- Information requiring more immediate response/action lends itself to email or fax.
- Indiscriminate use of the urgent/routine flags is at best very unhelpful.

3. What is the subject?

- A relevant email subject heading is essential and should be a clear concise indication of email content.
- It is preferable, even with brief emails, to assign a subject heading.

4. Who needs to know for reply or action and who just for information?

- "To:" addressees have responsibility to reply or act upon the content.
- "Cc:" addressees are purely for information and have no responsibility to reply/respond.
- It is important that all addressees can clearly see who sent the email and to whom. "Bcc:" addressees should be used sparingly.
- Frequently people send "blanket" emails without much thought, in case recipients may be interested. This is at worst laziness and often results in overload/duplication of information.
- It is preferable that, for multiple addressee messages, the addressee's names (both "to" and "cc") are clearly specified at the start of the text.

5. Reply or Forward buttons should be used carefully:

- Keep message relevant to subject heading.
- Restrict number of to-ings and fro-ings, generally once or twice is enough. The sense and relevance can soon become obscured/confused by too many back and forth emails.
- When forwarding it is often a good idea to add brief first line of text that explains why it is being forwarded and to whom.
- Often superfluous texts and addresses etc. can be deleted so making the actual message texts more apparent.

6. Housekeeping of your email application:

- Inboxes, Outboxes, Sent Items, Deleted Items should be kept tidy.
- When any email is actioned then move from Inbox to deleted box.
- Do a weekly/monthly monitor and clear out of Outboxes, Sent Items and Deleted Items.

7. Accuracy of email addresses:

- Accuracy of spelling, syntax and domain is of paramount importance.
- One letter wrong and email could go astray – even inside NHS net.

Internet

- You must not download programs from the Internet without permission from the Practice Manager or IT Administrator.

- Use of the Internet will be monitored.

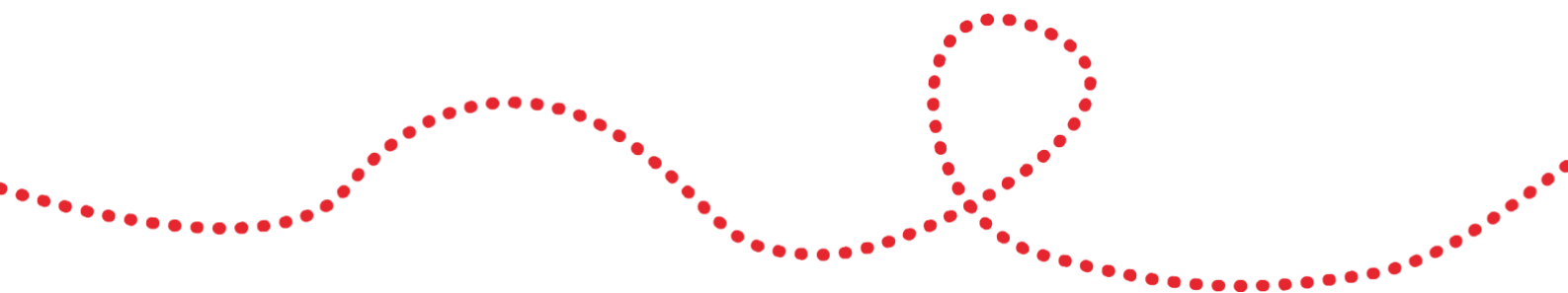
- Where accessing the Internet employees should act in a 'responsible manner'. Whatever applies in spirit to use of e-mail as described in Section 4 also applies to the Internet.

- Users must not access inappropriate or offensive Internet sites that are related to gambling, pornography, criminal skills, terrorism, cults, hate speech, illegal drugs, chain mail or anything not related to work issues. This list is illustrative, BUT NOT EXHAUSTIVE. Failure to comply may result in dismissal and may also constitute a criminal offence.

- Employees are forbidden from accessing social networking sites such as facebook, twitter, my space etc. in work time and under no circumstances should employees accept these sites for communication with patients/patient related issues as this could lead to a possible breach of confidentiality.

Auditing

- The surgery has the right at any time to audit any surgery property, be it a PC, portable computer, terminal, portable device, e-mail or paper. If there is evidence that the policy set out in this document has been contravened, the employee concerned may be subject to disciplinary procedures which could include dismissal. Any evidence that an employee has committed a criminal offence may be forwarded to the appropriate authorities for further action.



Correspondence, Reports and Results Protocol

Purpose

The purpose of the protocol is to set out the procedure for reviewing and acting on correspondence, reports and investigation results received at the practice. This protocol is relevant to anyone who works at the practice. This protocol will be reviewed annually to ensure it remains effective and relevant.

Background

For the welfare and safety of our patients it is crucial to process and act on correspondence, reports and results from outside the practice in a timely but safe manner. The information the practice receives can be from a variety of locations including hospitals, out of hours care providers and community health teams. The lawful basis on which this data is processed is that it is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional. (ICO category 9(2)(h) Overview of the GDPR).

Procedure

Correspondence, reports and investigation results from outside the practice may be received by fax, post or electronically. The detailed data mapping and how the Practice receives and sends data is available using the completed IG toolkit. https://www.igt.hscic.gov.uk/. This is updated each time the workflow is changed and is reviewed annually at a minimum.

INBOUND DATA FLOW

Paper correspondence/reports/results

1. When opening paper correspondence/reports/results received in the post, check and confirm addressee before opening.

2. Any paper correspondence /reports /results received by fax, post or patients must be given to a practice secretary who will scan the documents on the computer system and act on them accordingly.

3. The secretary must then electronically send the correspondence / report / results to the healthcare professional who referred the patient/ looks after the patient. Not every piece of data will go to the healthcare professional. An example of information they need to see are new diagnoses, referral requests, significant results etc.

4. The healthcare professional who receives the correspondence/report/results will decide what action to take, they will sometimes pass the work back to the secretaries if an additional administrative action is required.

5. The majority of correspondence/report/results need coding; therefore it is put into the queue for coding using the electronic clinical system.

6. After the correspondence/report/results are scanned into the patient's electronic record and no longer required, then the paper copy is shredded.

7. Any paper insurance reports, requests for medical records or medical forms are received, they should be filled out as fully as they can by the secretarial team and then passed to the GP to complete and check through. The name of the patient, company requesting the information and initials of the GP it is sent to will be entered in the blue reports book and ticked upon completion.

Electronic reports/results

1. Electronic reports/results are actioned by the GP who requested the investigation. The courses of action/comments are filed on the patient's electronic record. If there is any action to be taken then they will be passed to the reception/secretarial team to pass the message on to the patient.

2. Any urgent reports/results for a GP who is not on duty should be actioned by the duty doctor of the day. Routine reports/results are sent to the doctor who requested them. If a doctor is on leave/out of office the report/result is sent to any other doctor who has seen the patient.

3. All reports/results should be actioned on the day of receipt if possible.

4. When data comes via email, NHS mail should be used as much as possible. When emailing patients or outside agencies, the email address must be confirmed and you must have the patients consent/implied consent to send

the information across to them via email. For clarity, implied consent is when the patient initiates the email correspondence.

5. When data is received/sent via iGPR you must confirm the patients written consent is received before sending any information. If received, save a copy of the consent form onto the patients records. If not received, the request is rejected and it is up to the company requesting the information to chase and obtain written consent from the patient. Complete the electronic request as required and save a copy of the report onto the patient's records.

OUTBOUND DATA FLOW

Paper correspondence/reports/results

Any paper documents that need to go out of the practice will be sent out in the most secure way possible.

1. Paper documents that are sent on the internal mail should be in a sealed envelope with no patient information on show. Documents that need to be sent via Royal Mail or any other courier should be in a sealed envelope, stamped 'private and confidential'. If the documents inside the envelope are sensitive patient data then the envelope needs to be sent using recorded tracked post and the receipts kept in the folder for 6 months before destroying. Insurance reports, medical records and forms should always be sent using tracked secure post. If there is a charge for these a bill should be sent out and paid before any information is released. Any private fees for these should be entered on the private fees spreadsheet. This will help other colleagues so they do not duplicate work.

2. If there is any hand delivered correspondence/post to be transferred between Sandsend Surgery and Sleights Surgery, the information must be in a sealed bag and taken directly to the other site using a car as transport only.

3. Hand delivered items to patients such as post and prescriptions should be transferred straight from the surgery to their destination. They should be in a sealed addressed envelope stamped ‘private and confidential’. Staff members will be trusted not to lose information as they are undertaking a one off specific task. If the patient comes to collect the item at the surgery, their identification must be confirmed before receiving the item.

Electronic reports/results

1. A risk assessment must be carried out for each text and email that is sent out to patients to ensure that it is safe and secure to do so. Patient consent must be obtained before sending any information this way and email address and phone number must be verified. No block texts or emails including sensitive information should be sent out to the patient in this way.

2. When faxing information over, make sure that the fax is going to a safe haven and the fax number is confirmed and correct. Always use a fax cover sheet while faxing in case the information is intercepted.

3. Telephones must be used to transfer information as much as possible, this is because it is the most secure, confidential way and things will not get lost on their way in/out of the surgery. The correct number must be confirmed before using the telephone to transfer data; failure to do this might cause a breach in confidentiality. When giving or receiving results over the telephone, ensure that the information is confirmed and repeated back to the speaker.

DATA PROTECTION POLICY

INTRODUCTION

The Data Protection Act 1998 (DPA) requires a clear direction on Policy for security of information within the Practice. The policy will provide direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information. The following is a Statement of Policy which will apply.

THE POLICY

- The Practice is committed to security of patient and staff records.
- The practice will display a poster in the waiting room explaining to patients the practice policy
- The Practice will take steps to ensure that individual patient information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient's consent, unless otherwise legally compliant. This will include training on Confidentiality issues, DPA principles, working security procedures, and the application of Best Practice in the workplace.
- The Practice will undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.
- The Practice will maintain a system of "Significant Event Reporting" through a no-blame culture to capture and address incidents which threaten compliance.
- DPA issues will form part of the Practice general procedures for the management of Risk.
- Specific instructions will be documented within confidentiality and security instructions and will be promoted to all staff.

Signed:

Caldicott Guardian

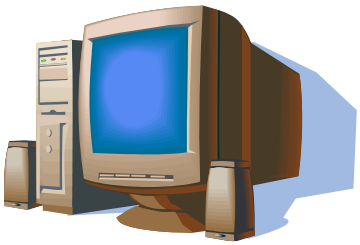
Practice Manager

Date:

Date:

PATIENT POSTER

DATA PROTECTION ACT – PATIENT INFORMATION



We need to hold personal information about you on our computer system and in paper records to help us to look after your health needs, and your doctor is responsible for their accuracy and safe-keeping. Please help to keep your record up to date by informing us of any changes to your circumstances.

Doctors and staff in the practice have access to your medical records to enable them to do their jobs. From time to time information may be shared with others involved in your care if it is necessary. Anyone with access to your record is properly trained in confidentiality issues and is governed by both a legal and contractual duty to keep your details private.

All information about you is held securely and appropriate safeguards are in place to prevent accidental loss.

In some circumstances we may be required by law to release your details to statutory or other official bodies, for example as part of a care quality commission inspection, if a court order is presented, or in the case of public health issues. In other circumstances you may

be required to give written consent before information is released – such as for medical reports for insurance, solicitors etc.

NHS England have also put a system in place to enable the NHS to use health information, sent from your record to a secure system, along with your postcode and NHS number, but not your name, where it can be linked with other health information. This allows those planning NHS services or carrying out medical research to use information from different parts of the NHS in a way which does not identify you. If you have any concerns or wish to prevent this from happening, please visit www.nhs.uk/caredata.

To ensure your privacy, we will not disclose information over the telephone or fax unless we are sure that we are talking to you. Information will not be disclosed to family, friends, or spouses unless we have prior written consent, and we do not leave messages with others.

You have a right to see your records if you wish. Please ask at reception if you would like further details.

INFORMATION GOVERNANCE POLICY

1. Summary

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2. Principles

The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Practice fully supports the principles of corporate governance and recognises its public accountability, but equally

places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The Practice also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Practice believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of everyone in the Practice to ensure and promote the quality of information and to actively use information in decision making processes.

There are 4 key interlinked strands to the information governance policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

2.1. Openness

- Non-confidential information about the Practice and its services should be available to the public through a variety of media, in line with the Practice's code of openness
- The Practice will establish and maintain policies to ensure compliance with the Freedom of Information Act
- The Practice will undertake or commission annual assessments and audits of its policies and arrangements for openness
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients
- The Practice will have clear procedures and arrangements for liaison with the press and broadcasting media
- The Practice will have clear procedures and arrangements for handling queries from patients and the public

2.2. Legal Compliance

- The Practice regards all person identifiable information, including that relating to patients as confidential
- The Practice will undertake or commission annual assessments and audits of its compliance with legal requirements

- The Practice regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- The Practice will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality
- The Practice will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)

2.3. Information Security

- The Practice will establish and maintain policies for the effective and secure management of its information assets and resources
- The Practice will undertake or commission annual assessments and audits of its information and IT security arrangements
- The Practice will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The Practice will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

2.4. Information Quality Assurance

- The Practice will establish and maintain policies and procedures for information quality assurance and the effective management of records
- The Practice will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- The practice will promote information quality and effective records management through policies, procedures/user manuals and training

3. Responsibilities

It is the role of the Senior Partner(s) in the Practice to define the Practice's policy in respect of Information Governance, taking into account legal and NHS requirements. The Senior Partner(s) is also responsible for ensuring that sufficient resources are available to support the requirements of the policy.

The designated Information Governance Lead in the Practice is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the Practice, raising awareness of Information Governance and ensuring that there is ongoing compliance with the policy and its supporting standards and guidelines.

The designated Information Governance Lead is responsible for overseeing the review of any breach of information governance procedure as a significant event. A review is to take place with all relevant staff, action is taken to ensure the breach is not repeated and the outcome communicated to all staff.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they remain aware of the requirements incumbent upon them for ensuring compliance on a day to day basis.

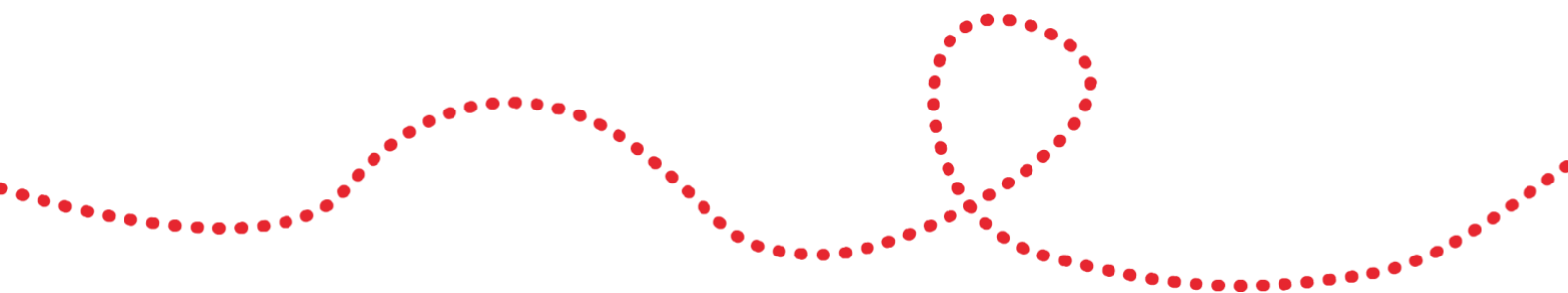
4. Policy Approval

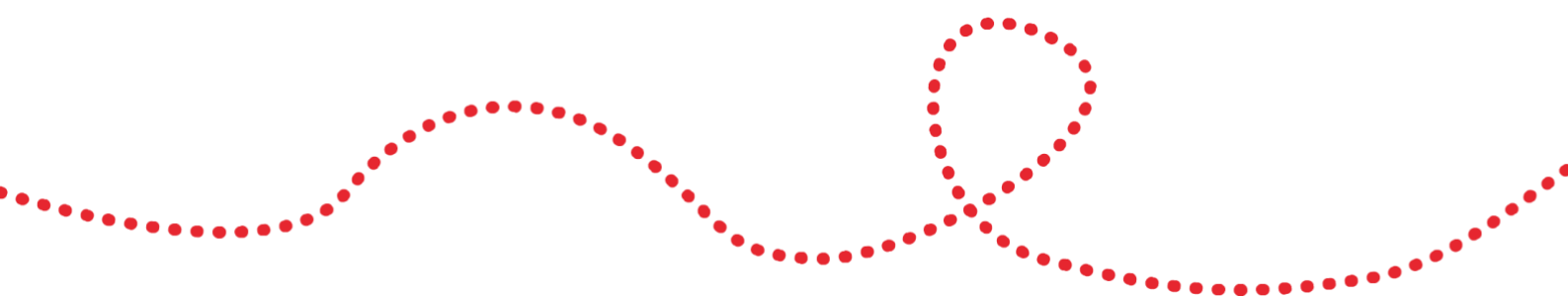
The Practice acknowledges that information is a valuable asset, therefore, it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all of its stakeholders.

We will, therefore, ensure that all staff, contractors and other relevant parties observe this policy in order to ensure compliance with Information Governance and

contribute to the achievement of the [insert organisation type] objectives and delivery of effective healthcare to the local population.

Partners name, signature and date:





Processing Personal Data Held on Staff

Staff Information and Consent Form

Central Dales Practice controls and processes personal data as part of its day to day function. To comply with the legal obligations relating to this activity, the practice must follow the guidelines laid out by the Information Commissioners Office (ICO) which includes The General Data Protection Regulation (GPDR). This regulation has been refined and there are some requirements that must be put in place by May 2018. One of the requirements is that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

To comply with the above, Central Dales Practice's policy and procedure is to:

- Inform all staff what information is held on them and how it is used.
- Collect only the data required to comply with our legal obligations.
- Hold data only for the legally required period (6 years after the staff member has left or their 75th birthday)
- Request any changes to personal information is communicated to the management team so that it is kept up to date.
- Hold personnel files in a securely locked, fire proof cabinet.

- Password protect any electronic documents which contain sensitive staff data. **Refer to Appendix A for details of personal data held.**

Sharing your personal data

We share some specific personal information if we are legally obliged to do so or employ a "data processor" to complete administrative tasks. Listed below is the information and who we share it with:

Information we share	Who we share it with	Why we share the information
Your application for the post	Your referees	To obtain employment references
Occupational Health form completed and signed by you	Occupational Health, York Trust	To ensure you are fit to work in the post
DBS form completed and signed by you	Processed online with uCheck https://www.ucheck.co.uk/	To ensure you do not hold a criminal record
NHS Pension status	Fairway Training Ltd Specialists in the NHS pension scheme	This company is paid by us to complete all our staff pension administration (excluding GPs)
Employment and tax status P45/P46 Real time monthly pay details	HMRC	To meet our legal obligation
Date of birth, National Insurance Number and gender	NHS Digital An NHS organisation	To meet our contractual obligation. Please note that you can give us a written request to opt out of this data sharing at any time.

Useful link for staff:

https://www.gov.uk/personal-data-my-employer-can-keep-about-me

Staff Member's Written Consent

I, the undersigned, confirm that I have read and understood this information document detailing what and why information is held about me and how this information is used.

I consent for Central Dales Practice to share information about me as detailed in the table above. I understand that I can give a written request to opt out of the data sharing for NHS Digital at any time. I can also request access to information held on me, to which Central Dales Practice must respond within 40 days.

Signed:

Dated:

Print name:

Appendix A: Personal Data Held On Staff:

Identity Checking

ID of new employees is checked and retained on their personnel file:

- Making sure all documentation is original, valid, current and, if possible, difficult to forge.
- ID can be accepted in an applicant's previous name if they cannot provide documentation in their new name but the individual should provide evidence (e.g. marriage/civil partnership certificate, decree absolute) of their name change.
- Secure **either** two forms of photographic personal ID and one document confirming address **or** two documents confirming address and 1 form of photographic ID.
- Making sure a copy of the individual's ID is taken for their personnel records. Ensure it is signed, dated and certified by the person taking the copy.
- ID checks apply to permanent staff, contractors and temporary staff. If the practice is using an agency, make sure they have followed the national standards and kept their operational policies up to date.

Right to Work Checks

The practice requests right to work documents where appropriate. Validate documents by making sure photos are of the individual, the date of birth is consistent across documents and appear consistent with the individual's appearance, check any expiry dates, check government stamped documents are actually giving the individual the right to work etc.

Professional Registration and Qualification Checks

Individual's registration with their relevant regulatory body, ie NMC or GMC. This is checked online.

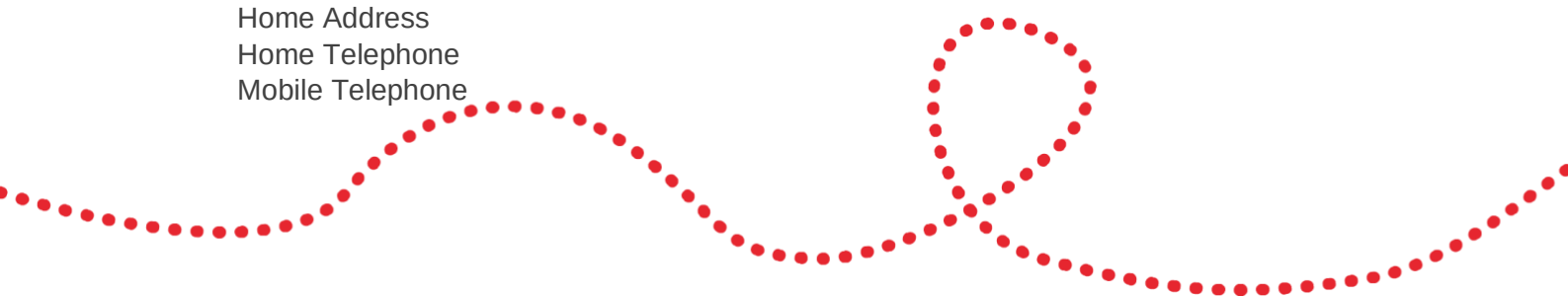
Original certificates seen and a copy kept on the personnel file.

Disclosure and Barring Service (previously CRB) Checks

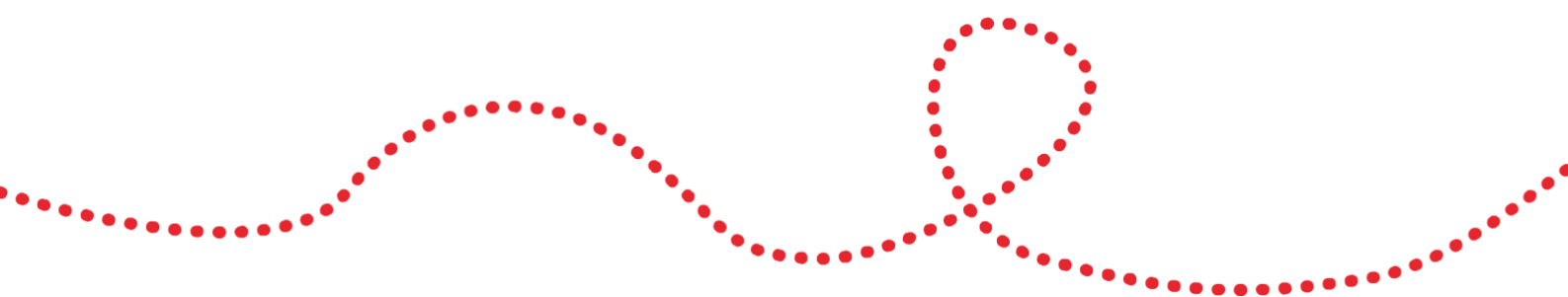
An enhanced DBS is requested for all clinical and non-clinical staff (for chaperoning).

Previous employment information
Curriculum Vitae and information on any employment gaps.
P45 or P46
Employment references

New Employment Information
Full Name
Date of Birth
Marital Status
Home Address
Home Telephone
Mobile Telephone



Next of kin details
E-mail
Date Employment Started
National Insurance No
Do you hold an Inland Revenue Certificate of Age Exception?
Bank Details
Medical Problems (e.g. Diabetic, Asthmatic)
Details of any disabilities which may prevent you from carrying out your duties or accessing certain areas of the surgery
Name and telephone number of GP
Signed employment contract
Occupational Health Details
Full immunisation update
Pension details / status
Training certificates / log
Smartcard details
DSE assessment



RECORDS RETENTION POLICY – ENGLAND

Based on Records Management Code of Practice for Health and Social Care 2016

Record	Retention period (years)	Comments
ACCIDENT REPORTS	10	Where litigation has been commenced, keep as advised by legal representatives.
Accounts - Annual (Final - one set only)	Permanent	CQC required period is 30 years
Accounts Minor records (pass books; paying-in slips; cheques counterfoils; cancelled/discharged cheques; accounts of petty cash expenditure; travelling and subsistence accounts; minor vouchers; duplicate receipt books and income records.	6	
BILLS, RECEIPTS AND CLEARED CHEQUES	6	
Buildings and engineering works, Inclusive of major projects abandoned or deferred - town and country planning matters and all formal contract documents (e.g. Executed agreements, conditions of contract, specifications, "as built" record		The general principle to be followed in regard to these records is that they should be preserved for the life of the buildings and installations to which they refer.

drawings and documents on the appointment and conditions of engagement of private buildings and engineering consultants.		
Building records (mortgage, transfers, disposal etc)	Permanent	
Buildings and PrSystmOnees – general maintenance records	3 years	
Cash Books	6	The Limitation Act, 1980
CCTV Images	31 days	Unless retention otherwise justified
Clinical Audit records	5	
Clinical System patient records	Permanent	Retain indefinitely for the foreseeable future
Complaints	10	Where litigations has been commenced, keep as advised by legal representatives

COMPUTERISED RECORDS	The recommended minimum retention periods apply to both paper and computerised records, though extra care needs to be taken to prevent corruption or deterioration of the data. Re-recording / migration of data will also need to be considered as equipment and software become obsolete. For guidance, see the Public Record Office guidance, Management and Appraisal of Electronic Records (1998) – see link below	
CONTRACTS	6	The Limitation Act, 1980
Death Certificates and death Records	2	
Diaries (office)	1	

EMPLOYMENT RECORDS – SEE PERSONNEL FILES AND PAYROLL RECORDS BELOW		
EQUIPMENT MAINTENANCE RECORDS	3	
ELECTRICAL TESTING RECORDS	3	
FIRE SAFETY RECORDS	5	
FREEDOM OF INFORMATION ACT REQUESTS	3	
FRIDGE TEMPERATURE RECORDS	1	
FUNDING DATA	6	
INSURANCE CERTIFICATES	40	
JOB ADVERTISEMENTS	1	
Job applications and descriptions (following termination of employment)	3	

MEDICAL GAS STORAGE, TRANSPORT AND SAFETY	3	
MINUTES OF MEETINGS	1	
OUT OF HOURS RECORDS	3	Where these are held as part of the clinical system the longer period of retention relating to clinical system records applies.
Paper Patient Records	20	20 years after last recording. 10 years after death. For patients treated under the Mental Health Act retain for 30 years after last recording.
Payroll / PAYE records	10	For superannuation purposes authorities may wish to retain such records until the subject reaches benefit age. Retain for 10 years after termination of employment
Personnel files (e.g. Personal files, letters of appointment, contracts references & related correspondence)	6	Keep for 6 years after subject of file leaves service, or until subject's 70th birthday, whichever is the later. Only the summary needs to be kept to age 70; remainder of file can be destroyed 6 years after subject leaves service.
Policies and Procedures (general operating policies)	3 years	Current version and all previous versions to be retained for a minimum 3 year period. % years recommended
Purchasing orders excluding medical devices and medical equipment	18 months	

Purchasing orders - medical devices and medical equipment	11 years	
Risk assessments	3	Retain three years and ensure that subsequent risk assessments are available
Rotas and staff duty rosters	4	4 complete years following the year to which they relate
Significant Event records	3	Including those to be notified to the CQC
Superannuation Forms (SD55)	10	
VAT Records	6	Complete years following the end of a VAT period
Water Safety records	5	

DoH guidance on records retention:

https://www.gov.uk/government/publications/records-management-nhs-code-of-practice

The Medical Protection Society recommend that any records not specifically mentioned elsewhere should be retained for 10 years after conclusion of treatment, the patient's death or after the patient has permanently left the country.

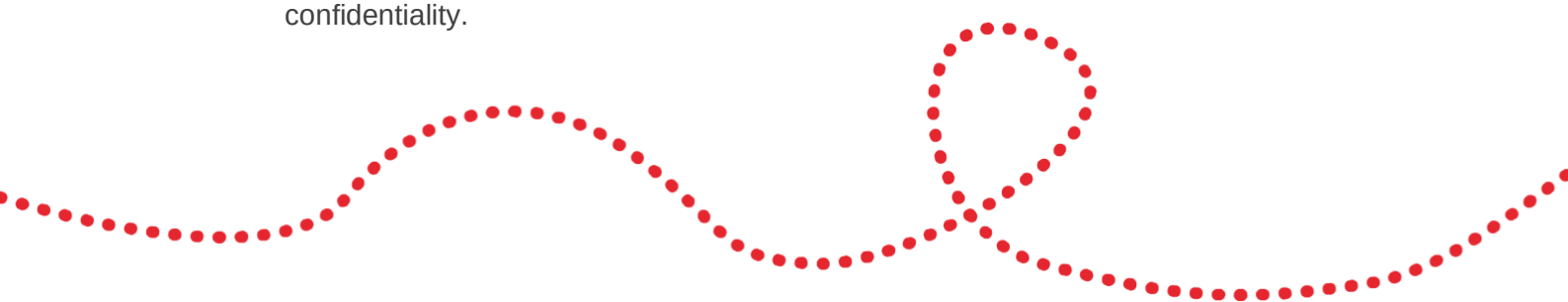
Business Link guidance on **employment** records retention

http://www.businesslink.gov.uk/bdotg/action/detail?type=RESOURCES&itemId=1074450470

SMARTCARD USAGE DECLARATION

I have been issued with a smartcard and confirm that I will comply with the following conditions:

1. agree that the smartcard issued to me is the property of the NHS. I understand it is for my use only and agree to use it only in the normal course of my employment;
2. agree that I will check the operation of my smartcard promptly after I receive it. This will ensure that I have been granted the correct access profiles. I also agree to notify my manager promptly if I become aware of any problem with my smartcard or my access profiles;
3. acknowledge that I will keep my smartcard private and secure and that I will not permit anybody else to use it or any session established with the NHS Care Records Service applications. I will not share my passcodes with any other user. I will not make any electronic or written copies of my Passcodes (this includes function keys). I will take all reasonable steps to ensure that I always leave my workstation password protected. If I lose my smartcard or if I suspect that it has been stolen or used by a third party I will report this to my manager as soon as possible;
4. The smartcard is to be kept under my personal control at all times and must not be left inserted into a smartcard reader when I am not present;
5. On leaving a terminal the Smartcard is to be removed. However, it is recognised that this may not be practical on every occasion in the dispensing/reception area as staff have the need to sometimes use more than one terminal.
6. Staff members sharing Smartcards on more than one occasion will be considered for disciplinary action in accordance with the Practice's normal procedures. This would normally be after an informal warning
7. agree that I will only use my Smartcard, the NHS Care Records Service applications and all patient data in accordance with The NHS Confidentiality Code of Practice (as available on the **www.dh.gov.uk** site) and (where applicable) in accordance with my contract of employment and with any instructions relating to the NHS Care Records Service applications which are notified to me;
8. agree not to maliciously alter, neutralise, circumvent, tamper with or manipulate my Smartcard, NHS Care Records Service applications components or any access profiles given to me;
9. agree not to deliberately corrupt, invalidate, deface, damage or otherwise misuse any NHS Care Records Service applications or information stored by them. This includes but is not limited to the introduction of computer viruses or other malicious software that may cause disruption to the services or breaches in confidentiality.



10. acknowledge that my smartcard may be revoked or my access profiles changed at any time without notice if I breach this Agreement; if I breach any guidance or instructions notified to me for the use of the NHS Care Records Service applications or if such revocation or change is necessary as a security precaution. I acknowledge that if I breach this Agreement this may be brought to the attention of my employer who may then take appropriate action (including disciplinary proceedings and/or criminal prosecution);
11. acknowledge that my employer shall notify the Registration Authority at any time should this Agreement be terminated and to have my Smartcard revoked e.g. on cessation of my employment with health care organisations or other relevant change in my job role; and
12. acknowledge that these terms and conditions form a binding Agreement between myself and those organisations who have sponsored my role(s). I agree that this Agreement is governed by English law and that the English courts shall settle any dispute under this Agreement.

Signed: ……..

Print name: ……

Date: ……

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.[8]

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:
To meet legal requirements under: Employment law Equality law HMRC regulations Pension legislation To meet contractual requirements: GMS contract ICO "Overview of the General Data Protection Regulation (GDPR)" reference: 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract 6(1)(c) – Processing is necessary for compliance with a legal obligation In relation to employee data and 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional For the patient data held.

WHO – whose personal data is processed?
Having identified why personal data is processed, use those reasons to determine whose personal data is processed.

[8] GDPR Article 4 Definitions

Personal data may be processed for the following data subjects:	
Staff	**Patients**
• Current / former • Associated (Health visitors / pharmacists / physiotherapists / counsellors) • 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:
As above

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 (GMS) • Legitimate interest of the data controller

List what personal data is processed:

Staff:
Refer to Processing Personal Data Held on Staff; Staff Information and Consent Form on page 40.

Patients:
As above

Details of healthcare information has been entered onto the Information Governance Toolkit:

https://www.igt.hscic.gov.uk/

This toolkit identifies the risk level for each process.

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**
• In accordance with the current retention schedule – (use PI retention schedule)	• In accordance with the current retention schedule – (use PI retention schedule)

List when personal data is processed:		
Obtained / updated	**Disclosure (with who & why)**	**Retention period**
All data is normally processed on the day of receipt not withstanding delays due to staffing issues or workload levels. Refer to the Retention policy on page 45		

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 in fireproof locked cabinets • Staff files • Hard copies of prescriptions etc. • Administration offices	• Locally established databases • SYSTMONE Web	• Fixed • Portable (laptops) • Remote servers • Cloud • Intranet
Asset register:		

Annex B – The Data Protection Impact Assessment

This document is to be used to conduct a DPIA at Central Dales Practice.

Step 1 – Determining the need

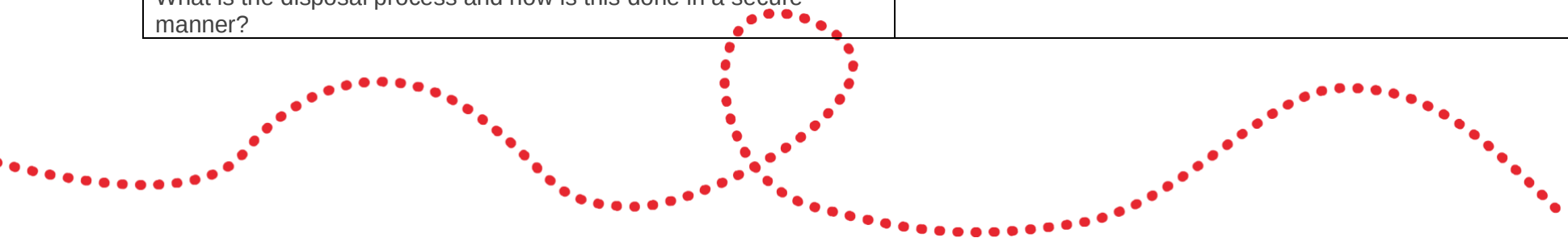
DOES THE PROCESS INVOLVE ANY OF THE FOLLOWING:	YES	NO
The collection, use or sharing of existing data subjects' health information?		
The collection, use or sharing of additional data subjects' health information?		
The use of existing health information for a new purpose?		
The sharing of data subjects' 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. There is no stipulated format for the report; each practice can amend as they deem necessary.

Step 5 – Reviewing the DPIA

The review process is detailed in the report.

Data Protection Impact Assessment Report

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

Overview:

Central Dales Practice 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 Central Dales Practice 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 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 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 (SYSTMONE 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).