# Data Security & Protection Policy

## Document Control

### A. Confidentiality Notice

This document and the information contained therein is the property of Arch Health CIC.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Arch Health CIC.

### B. Document Details

| | |
|---|---|
| **Classification:** | Data Security & Protection |
| **Lead Director:** | Dr Tim Worthley, Clinical Lead |
| **Organisation:** | Arch Health CIC |
| **Document Reference:** | Data Security & Protection Policy (including appointment of Caldicott Guardian) |
| **Current Version Number:** | V1.3 |
| **Current Document Approved By:** | Tim Worthley |
| **Date Approved:** | 17/5/18 |
| **Ratified by Arch Board:** | 22.05.2018 |
| **Renewal Due Date (yearly review):** | 01.05.2019 |

### C. Document Revision and Approval History

| Version | Date | Version Created By: | Version Approved By: | Comments |
|---|---|---|---|---|
| 1.2 | 18/08/2017 | Olivia Hind | TW | Amended with review of all policies. Changed formatting and blended with duplicate policy. |
| 1.3 | 17/5/18 | FP | TW | GDPR updates & full policy review |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |

## 1. INTRODUCTION

Arch Health CIC handles ever-increasing amounts of information. Timely and accurate information is crucial both for the clinical decision-making and 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 that information is efficiently managed by Arch, and that we have appropriate policies and procedures to provide a robust framework for data protection and security.

Arch must be able to demonstrate compliance with the GDPR and Data Protection Act 2018 at all times. Understanding the requirements of the GDPR and Data Protection Act 2018 will ensure that personal data of patients, staff, contractors, locums, students including those carrying out work experience or work placements, and is protected accordingly.

## 2. SCOPE

2.1 Who it applies to

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

2.2 Why and how it applies to them

All personnel at Arch have a responsibility to protect the information they process. This document has been updated to enable all staff to understand their individual and collective responsibilities in relation to the GDPR and Data Protection Act 2018.

Arch 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.

## 3. DEFINITION OF TERMS

3.1 Data Protection Act

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

3.2 Data Protection Officer

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

3.3 Data Protection Authority

National authorities tasked with the protection of data and privacy.

3.4 Data Controller

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

3.5 Data Processor

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

3.6 Data Subject

A natural person whose personal data is processed by a controller or processor. This can include: patients, staff, contractors, locums or job applicants, students including those carrying out work experience or work placements. Please note this list is non-exhaustive.

3.7 Personal data

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

3.8 Processing

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

3.9 Recipient

The entity to which personal data is disclosed.

3.10 Privacy Notice

Is a statement or document that discloses some or all of the ways a party gathers, uses, discloses, and manages a data subject's information. It fulfils a legal requirement to protect a data subject's privacy.

## 4. THE SIX DATA PROTECTION PRINCIPLES

Personal data should be processed in accordance with the six Data Protection Principles for GDPR identified by the ICO, which means data will:

• Be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
• Be processed fairly, lawfully and transparently;
• Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
• Be collected and processed only for specified, explicit and legitimate purposes;
• Not be kept for longer than is necessary for the purposes for which it is processed;
• Be processed securely.

## 5. TYPES OF DATA HELD

**5.1 As an employer:** Arch has to hold certain amounts of personnel data, including personal data relating to its employees, contractors including locums, students and work experience placements, in order for the organisation to function effectively. This may include information that identifies individuals by reference to their names, job titles, responsibilities or other matters related to the operation of the organisation. It also temporarily holds personal data of unsuccessful job applicants but this is destroyed or deleted as soon as the recruitment process is over.

Personal data, including some sensitive data, likely to be found on an employee's file could be:

- Name, address, telephone number
- Education and training information
- Interests/Hobbies
- Employment history (including reason for leaving)
- Experience (skills/knowledge etc)
- Whether the applicant has ever been convicted of a criminal offence
- Referee details (references are kept on file)
- Equal Opportunities form
- Original application form/interview notes
- Appraisal forms
- Vehicle information
- Training undertaken and required
- Next of kin name and contact details
- Contract and updates to the contract including salary changes (together with notification of this)
- Salary and pension information
- National insurance number
- Bank account details
- Sickness record
- Vaccinations record
- Any complaint or grievance action involving the staff member
- Responses from DBS checks

Some of the information above will also likely be requested, stored and processed of contractors - locums in particular.

As part of their Terms and Conditions of employment, all employees must:

- Check that any personal data that they have provided to Arch Health CIC is accurate and up to date
- Inform Arch Health CIC of any changes to information which they have provided e.g. change of address

**Please find Arch's Employee Privacy Notice here**

**5.2 As a healthcare provider:** Arch holds data and information relating to patients and their health and has a duty to protect this in line with the Caldicott Guardian principles.

Arch Health CIC's Medical Director is the appointed Caldicott Guardian. Roles and responsibilities of this post are described in the Information Governance Framework and Policy.

- The Caldicott Policy applies to all patient-identifiable information, regardless of whether it is of a medical nature or not, obtained and processed by the Practice.
- This document:
  - Sets out the Practice's policy for the protection of all patient-identifiable information obtained and processed.
  - Establishes the responsibilities for Caldicott Guardianship.
  - Provides reference to the Caldicott principles.

The below approach applies to all patient-identifiable information processed, stored on computer or relevant filing systems (manual records) and the Practice staff who use the information in connection with their work.

It also follows the guidelines suggested in the revised version of the GMC document "*Raising and acting on concerns about patient safety*", effective 12 March 2012, a copy of which can be downloaded here:

http://www.gmc-uk.org/Raising_and_acting_on_concerns_about_patient_safety_FINAL.pdf_47223556.pdf

Patient-identifiable information takes many forms. It can be stored on computers, transmitted across networks, printed or stored on paper, spoken or recorded.

The Practice will take all necessary steps to safeguard the integrity, confidentiality, and availability of sensitive information.

No staff member employed by the Practice (including temporary or agency staff) is allowed to share any patient-identifiable information unless it has been authorised by the Practice's Caldicott Guardian.

The Medical Director is the Caldicott Guardian and Data Protection Officer at Arch Health CIC.

It is unlikely that any authorisation to share patient-identifiable data will be granted unless the access is on a need to know basis and justifiable against the Caldicott principles.

The Caldicott standard is based on the following six principles:

- **Justify the purpose(s)** - Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.
- **Don't use patient-identifiable information unless it is absolutely necessary** - Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
- **Use the minimum necessary patient-identifiable information** - Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
- **Access to patient-identifiable information should be on a strict need-to-know basis** - Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
- **Everyone with access to patient-identifiable information should be aware of their responsibilities** - Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
- **Understand and comply with the law** – Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

## 6. ACCESS

6.1 Data subject's personal data and access rights

Personal data is any information identifying a data subject (a living person to whom the data relates). This could be a patient, member of staff, contractor, locum, job applicant, student including those carrying out work experience or work placements. It includes information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers the Practice possesses or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. It does not include anonymised data, but does include any expression of opinion about the person, or any indication of the intentions of the Practice or others, in respect to that individual.

All data subjects, including patients and staff, have a right to access their data and any supplementary information held by Arch. Arch ensures that all Arch Healthcare patients, staff, contractors, locums or job applicants, students including those carrying out work experience or work placements, are aware of their right to access their data and have produced and publicised Privacy Notices to demonstrate some or all of the ways we gather, use, disclose, and manage a data subject's information.

For more information on Subject Access Requests please see our policy here.

## 6. DATA BREACHES

6.1 Data breach definition: A data breach is defined as any incident that has affected the confidentiality, integrity or availability of personal data.

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

If any data breach takes place all staff must:

- Log the incident on the Significant Events Reporting System.
- If considered a serious breach – inform the Practice Manager who will coordinate an investigation to assess the seriousness of the incident. If required, this will be reported to the Caldicott Guardian/DPO, Commissioners, the CCG and the Information Commissioner's Office.

Any learning from incidents will be shared with the staff team.

6.2 Reporting a data breach to the ICO

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.

The data controller is to ensure that all breaches at Arch are recorded; this includes:
• Documenting the circumstances surrounding the breach
• The cause of the breach; was it human or a system error?
• Identifying how future incidents can be prevented, such as training sessions or process improvements

6.3 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 Arch 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

## 7. DATA ERASURE

7.1 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

7.2 Notifying third parties about data erasure requests

Where Arch 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. Please note, this policy will be updated once the NHS IGA have issued guidance regarding data erasure.

## 8. CONSENT

8.1 Appropriateness

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

8.2 Obtaining consent

If it is deemed appropriate to obtain consent, the following must be explained to the data subject:
• Why the practice wants the data
• How the data will be used by the practice
• The names of any third-party controllers with whom the data will be shared
• Their right to withdraw consent at any time

All requests for consent are to be recorded, with the record showing:
• The details of the data subject consenting
• When they consented
• How they consented
• What information the data subject was told

Consent is to be clearly identifiable and separate from other comments entered into the healthcare record.

For more information please see our Consent Policy here.

8.3 Parental consent

Currently GDPR states that parental consent is required for a child under the age of 16, however, the DPA18 will reduce this age to 13 in the UK. And this policy will be reviewed at that point. Additionally, the principle of Gillick competence remains unaffected; nor is parental consent necessary when a child is receiving counselling or preventative care.

8.4 Staff consent

Arch Health CIC cannot hold sensitive data on an employee's file without their consent. It is essential therefore that when dealing with medical issues, for example, consent for access to medical records, is obtained from the employee. There are exceptions to this stipulation which include when the organisation must hold sensitive data:

- In accordance with legal obligations e.g. Health and Safety requirements
- To protect the employee's interests
- For the purposes of defending a complaint of unlawful discrimination on the grounds of sex, race, union membership etc
- For the purpose of maintaining and monitoring Arch Health CIC Equality Policy

## 9. SECURITY & STORAGE INCLUDING DATA MAPPING

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage and that both access and disclosure must be restricted. All employees are responsible for ensuring that:

- Any personal data which they hold is kept securely e.g locked storage facilities, use of passwords etc

- Personnel information is not disclosed either orally, in writing or otherwise to any unauthorised third party or inappropriate work colleague

Arch Health CIC is committed to ensuring the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information as laid down by the Disclosure & Barring Service for all staff using the Disclosure & Barring Service to help assess the suitability of applicants for positions of trust, both as paid employees and volunteers.

Disclosure information is only passed to those who are authorised to receive it in the course of their duties and it is only used for the specific purpose for which it was requested and for which the applicant/employee's full consent has been given.

In order to have an accurate understanding of where personal data is kept, and in what format, Arch has carried out a GDPR compliant Data Mapping Exercise which will be reviewed regularly. 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.

## 10. DATA PROTECTION IMPACT ASSESSMENTS:

It is important that changes to services and systems and processing of person identifiable data are assessed to ensure that confidentiality, accessibility and integrity of data are maintained. The practice will liaise with DPO to identify when Data Protection Impact Assessment (DPIA) is required and will ensure this is completed and approved before changes are introduced.

The relevant legislation and policy frameworks associated with this policy are outlined in Appendix 1. Regular updates to this policy will be applied when further information and/or direction is received.

## 11. TRAINING, POLICIES AND PROCEDURES

Arch takes their responsibility for the security and protection of all identifiable personal data very seriously.

All Practice staff have responsibility for compliance with this policy. To this end the Practice has:

- ➢ Confidentiality clauses in each employee's employment contract;
- ➢ An e-learning package (including a competency test);
- ➢ An Employee Handbook (outlining employee responsibilities);
- ➢ Policies, procedures and agreements to ensure any transfer of patient-identifiable information is compliant;
- ➢ No-blame culture to capturing and addressing incidents which threaten compliance via Arch's Significant Event Reporting procedure
- ➢ Data Protection issues form part of the Practice general procedures for the Management of Risk including the Arch Board Risk Register

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.

Arch Health Community Interest Company is registered with the ICO. Registration number: ZA215866

## Appendix 1 – Compliance Acts

The Practice adheres to the following Acts:

### Data Protection Act 2018 - Data Protection Principles

Information held must be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of identifiable personal data and against accidental loss or destruction of, or damage to, identifiable personal data.

Identifiable personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of identifiable personal data.

## GDPR - General Data Protection Regulation 2018

The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018.

## The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access.

Each organisation will issue an individual user id and password to each employee which will only be known by that individual and must not be divulged to, or misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities.

Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

## The Access to Health Records 1990

This Act gives patients' representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991.

This Act is only applicable for access to deceased patient's records. All other requests for access to information about living individuals are provided under the access provisions of the Data
Protection Act 1998.

## Access to Medical Reports Act 1988

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

## Confidentiality: NHS Code of Practice

Gives NHS bodies guidance concerning the required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records. It is a key component of information governance arrangements for the NHS.