Dated: 17/05/2023

Reviewed by: Dr Nicholas Lowe, Rebecca Ellery

Data Protection Policy the Caldicott Principles and Confidentiality Policy

This policy sets out the framework to ensure that the Highfield Health complies with the law.

Data Protection Act - Principles and Practices to ensure compliance

Highfield Health will put in place procedures to ensure the eight principles in the DPA are met.

Principle 1 - Personal data shall be processed fairly and lawfully

Compliance will be achieved by implementing the following measures:

- Ensuring the Highfield Health's Data Protection Notification is kept up to date. Complying with the common law duty of confidentiality; that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual. However the law recognises that research which does not directly lead to decisions about a person should have special freedom to use information in ways not foreseen when it was collected but these uses must be fair and lawful. *(Taken directly from MRC Executive Summary – Personal Information in Medical Research)*
- Ensuring that certain conditions in Schedules 2 and 3 of the Act are met (see Appendix 2 for detail of the Data Protection Act - First Principle). Informing the individual how the data will be processed. This means fully describing how the data will be used i.e. what will be done to the data; for what purposes it will be used, who it will be passed onto, how it will be processed, stored and destroyed.

Principle 2 - To obtain personal data only for specified and lawful purposes and further process it only in a compatible manner

The following must be adhered to:

- Personal data must only be processed for the purposes for which it was originally obtained.
- Protocols should be in place to ensure that personal data that is passed on is used only for the purposes for which it was originally obtained.

- Hospitals and practices involved in research must develop procedures for making patients aware that their information may sometimes be used for research, and explaining the reasons and safeguards. Any objections from patients must be respected. (*from MRC Executive Summary – Personal Information in Medical Research)*

Principle 3 - Personal data must be adequate, relevant and not excessive

This will be achieved by:

- Conducting routine audits as part of good data management practice
- Ensuring that relevant records policies and professional guidelines, i.e. information lifecycle, are adhered to.

Principle 4 - Personal data must be accurate and up to date

This will be achieved by:

- Data users recording information accurately and taking reasonable steps to check the accuracy of information they receive from data subjects or anyone else.
- Data users regularly checking all systems to destroy out-of-date information and correcting inaccurate information.

Principle 5 - Personal data must be kept no longer than necessary

This will be achieved by:

- Adherence to Information Management Policies (i.e. information lifecycle)
- Staff working in joint team situations using the maximum retention period.
- Compliance with the Department of Health's Records Management: NHS Code of Practice. Part 2 provides a comprehensive retention schedule, which is reflected in the information lifecycle policy

Principle 6 - Personal data must be processed in accordance with the rights of the Individual

The Act gives seven rights to individuals, they are a:

- right of subject access (e.g. to see or have a copy of your medical records or staff files)
- right to prevent processing likely to cause damage or distress
- right to prevent processing for the purposes of direct marketing
- rights in relation to automated decision taking
- right to take action for compensation if the individual suffers damage
- right to take action to correct, block, erase or destroy inaccurate data
- right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

Should an individual make a request to prevent processing then depending on the individual circumstances, Highfield Health would have to make a judgement based on the risk to the individual or others whether it was right to provide a service. This decision can only be made by the Caldicott Guardian.

Principle 7 - Personal data must be kept secure

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

Principle 8 - Personal data shall not be transferred to a country outside the European Economic Area unless that country can ensure adequate level of protection

To ensure compliance protocols must be in place for the transfer of personal data outside the European Economic Area unless that country can ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Caldicott Principles for handling personal confidential data:

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate Guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data 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).

3. Use the minimum necessary personal confidential data

Where the use of personal confidential data 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.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one information flow is used for several purposes. Health care organisations should be aware of the research conducted within the organisation, and should ensure research teams are accountable to them (*from MRC Executive Summary – Personal Information in Medical Research).*

5. Everyone with access to personal confidential data should be aware of their responsibilities

The organisation must ensure that those handling personal confidential data, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Understand and comply with the law

Every use of personal confidential data must be lawful. The Caldicott Guardian is responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality

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

Confidentiality

The 'Confidentiality: NHS Code of Practice' was published by the Department of Health following major consultation in 2002/2003. The consultation included patients, carers and citizens; the NHS; other health care providers; professional bodies and regulators. The guidance was drafted and delivered by a working group made up of key representatives from these areas.

The Code of Practice is a guide to required practice for those who work within or under contract to NHS organizations concerning confidentiality and patients' consent to the use of their health records. This document uses the term 'staff' a convenience to refer to all those to whom this code of practice should apply. Whilst directed at NHS staff, the Code is also relevant to any one working in and around health services. This includes local authority staff working in integrated teams and private and voluntary sector staff.

This document:

- introduces the concept of confidentiality;
- describes what a confidential service should look like;
- provides a high level description of the main legal requirements;
- recommends a generic decision support tool for sharing/disclosing information;
- lists examples of particular information disclosure scenarios

The full document **CONFIDENTIALITY: NHS CODE OF PRACTICE** can be accessed from http://www.dh.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/PublicationsPolicyAndGuidanceArticle/fs/en?CONTENT_ID=4069253&chk=jftKB%2B

Also available is the **Supplementary Guidance: Public Interest Disclosures** – published in November 2010 which provides guidance to NHS staff in making what are often difficult decisions on whether a breach of patient confidentiality can be justified in the public interest.

Following the publication of the *Caldicott Review in March 2013*, the Health & Social Care Information Centre published "A guide to confidentiality in health and social care" which identified five rules for treating confidential information with respect:

Rule 1:
Confidential information about service users or patients should be treated confidentially and respectfully

Rule 2:
Member of a care team should share confidential information when it is needed for the safe and effective care of an individual

Rule 3:
Information that is shared for the benefit of the community should be anonymised

Rule 4:
An individual's right to object to the sharing of confidential information about them should be respected

Rule 5:
Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed

For the full document, which contains helpful guidance – go to:
http://www.hscic.gov.uk/confguideorg

5.1 Patient Confidentiality

Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

On admission and/or on first contact with the service for a particular matter, all patients should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, and those they specifically do not give permission to receive information. This information must be recorded in the clinical records.

In cases where relatives have been heavily involved in patient care, the patient must be explicitly asked as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed

As a research active organisation staff might screen patients' records to identify any potential research participants with the lead clinician's permission. Patients may also be approached by staff regarding participation in a particular research study in order to obtain consent.

In the event of the patient being unable to give permission the Mental Capacity Act 2005 must be followed. Staff should refer to the Mental Capacity Act Policy and procedures for detail.

In all cases, the wishes expressed must be appropriately documented in the patient's clinical records.

Staff Confidentiality

All staff is required to keep confidential any information regarding patients and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications should be conducted in a confidential manner.

Confidential information must not be disclosed to unauthorized parties without prior discussion and confirmation with a senior member of staff. Staff must not process any personal information in contravention of the Data Protection Act.

Any breaches of these requirements will potentially be regarded as serious misconduct and as such may result in disciplinary action.

All staff have a confidentiality clause in their contract of employment.

Exemptions to the Data Protection Act

In certain circumstances personal information may be disclosed and guidance is below. However it is vital in each case that staff make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason.

Disclosing Information against the Subject's wishes

The responsibility to withhold or disclose information without the subject's consent lies with the senior manager or senior clinician involved at the time and cannot be delegated.

Circumstances where the subject's right to confidentiality may be overridden are rare. Examples of these situations are:

- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision
- Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs
- Where there is a serious threat to the healthcare professional or other staff
- Where there is a serious threat to the community
- In other exceptional circumstances, based on professional consideration and consultation.

The following are examples where disclosure without consent is required:

- ✓ Births and deaths - National Health Service Act 1977
- ✓ Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984
- ✓ Poisonings and serious accidents at the work place - Health & Safety at Work Act 1974
- ✓ Terminations - Abortion Regulations 1991
- ✓ Child abuse - Children's Act 1989 and The Protection of Children Act 1999
- ✓ Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
- ✓ Road traffic accidents - Road Traffic Act 1988
- ✓ Prevention/detection of a serious crime e.g. terrorism, murder - The Crime and Disorder Act 1998

If in doubt, staff should seek guidance, in confidence, from the senior Clinician or the appropriate Senior Manager or the Information Governance Manager or the Caldicott Guardian. **Dr N Lowe and Rebecca Ellery (Practice Manager)**

Highfield Health will support any member of staff who, after using careful consideration, professional judgement, and has sought guidance from their manager, can satisfactorily justify and has documented any decision to disclose or withhold information against a patient's wishes.

Non–Disclosure of personal information contained in a health record

An individual requesting access to their health records may be refused access to parts of the information if an appropriate clinician deems exposure to that information could cause physical or mental harm to the data subject or a third party. Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure must be documented.

Where access would disclose information relating to or provided by a third party, consent for release must be sought from the third party concerned, unless that third party is a health professional who had provided the information as part of their duty of care. Where the third party does not consent, the information may be disclosed provided the identity of the third party is not revealed. The DPA suggests that this might be done by omitting names and identifying particulars from the records. Care should be taken to ensure that the information if released is genuinely anonymous.

Further guidance is available from the SIRO

Highfield Health is not required to supply copies of health records if the individual requesting the information has:

- not provided enough supporting information in order for the information to be located
- not supplied the appropriate fee
- not supplied the necessary evidence of identity

or

- the retrieval of the health records requires disproportionate effort

The Information Commissioner has released guidance on issues of law concerning the right of access to personal data. See **Durant v Financial Services Authority [2003] EWCA Civ 1746, Court of Appeal (Civil Division), decision of Lord Justices Auld, Mummery and Buxton dated 8th December 2003 (**http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialistguides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf **)** which gives guidance on

- what makes “data” “personal” within the meaning of “personal data”
- what is meant by a “relevant filing system”

- upon what basis should a data controller consider it "reasonable in all the circumstances" to comply with the request even though the personal data includes information about another and that other has not consented to disclosure

Personal Identifiable Data in Medical Research

In order to ensure the key principles of Data Protection Act are adhered to, The Medical Research Council published guidelines on Personal Information in Medical Research (2000). It clearly states that the law assumes that whenever people give personal information to health professionals caring for them, it is confidential as long as it remains personally identifiable.

Frequently during medical research personal information is obtained from surveys, medical records, scientific tests and interviews. This information is confidential and any failure to control the ways in which it is used could be potentially harmful to a person's sense of security and self-confidence, the doctor-patient relationship or lead to unfair discrimination.

Since The Data Protection Act (DPA, EU Data Protection Directive 95/46/EC) became law in 2000 researchers must also ensure their work is consistent with the law. However the law recognises that research which does not directly lead to decisions about a person should have special freedom to use information in ways not foreseen when it was collected but these uses must be fair and lawful.

All research within Highfield Health must comply with the Data Protection & Caldicott Guardian Principles as set out within this Policy, be registered by the Research and Outcomes Department and undergo review by the SIRO.

The Information Governance Manager will maintain a database of all Data Protection approval requests as evidence for compliance with the DPA registration and Information Governance Toolkit.

Privacy Impact Assessment Procedure and Template

All projects and processes that involve personal information or intrusive technologies give rise to privacy issues and concerns. To enable Highfield Health to address the privacy concerns and risks a technique referred to a Privacy Impact Assessment (PIA) must be used. This process ensures that Highfield Health complies with the Data Protection Act: Principle 1 – *"Personal Data shall be processed fairly and lawfully"* and Principle 2 – "*Personal Data shall be processed for a specified purpose".*

Monitoring Compliance

Data Protection Act Compliance:

Compliance with the Data Protection Act is mandatory and Highfield Health will ensure that it keeps an up to date register of all purposes for processing personal data and makes the required notification with the Information Commissioners Office.

Policy Review

This policy will be subject to regular planned review and, if revised, all staff will be alerted to the new version.