POLICY POL2/4

Confidentiality and Data Protection Policy

This Policy replaces POL2/3	**Copy Number**
	Effective **08/07/19**

Summary of Significant Changes

Redrafted to reflect legislation change, Data Protection Act 1998 replaced by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. No shading as significant change.

Policy

NHS Blood and Transplant (NHSBT) will develop, implement and maintain technical and organisational measures to protect the privacy of all individuals, living or deceased, about whom it holds information. It will achieve and maintain compliance with all applicable common law and statutory requirements, and sector best practice. These include but are not limited to the General Data Protection Regulation, Data Protection Act 2018, the Access to Health Records Act 1990, the NHS Confidentiality Code of Practice, and the reports of the National Data Guardian

Purpose

This document outlines the responsibilities, processes and procedures in place to ensure that the privacy and confidentiality of donors, patients, employees and other supporters of NHSBT are respected and maintained.

Responsibilities

Responsibility for compliance with this policy exists at all levels throughout NHSBT but legal accountability rests with the Chief Executive. Specific responsibilities are delegated to groups or posts as detailed within this policy, NHSBT's overarching Information Governance policy, or related documents.

The Information Governance Manager is responsible for maintaining NHSBT's notification to the Information Commissioner's Office (ICO), as required under the Data Protection Act 2018.

The Information Governance Committee (IGC) is responsible for review and approval of this policy.

Definitions

A glossary of terms and definitions routinely used in data protection is given as an appendix to this document.

Applicable Documents

POL266	NHSBT Information Governance
POL10	NHSBT Information Security Policy
MPD11	Handling of Data Protection Subject Access Requests

SPN189	NHSBT Record Storage
MPD1006	Conducting Data Protection Impact Assessment
POL209	Information Governance Training
POL247	Patient Registration for Transplantation
INF1352	Guidance on Whether and How to Share Information
	NHSBT Code of Conduct
	NHSBT Disciplinary Policy and Procedure
	Confidentiality: NHS Code of Practice
	'To Share or Not to Share?' The Information Governance Review (Caldicott 2) Appendix 5 for definition of personal data

Introduction

NHS Blood and Transplant (NHSBT) is a Special Health Authority within the NHS. It manages the national voluntary donation system for blood, tissues, organs and stem cells turning these precious donations into products that can be used safely to the benefit of the patient. It also provides a range of specialist laboratory services.

In the course of its operations, NHSBT must collect, hold, use and create information about identifiable individuals. When such individuals are living, NHSBT must observe its obligations and the individuals' rights under the General Data Protection Regulation (GDPR) and Data Protection Act 2018. Common law duties of confidentiality also apply, as in the exchange of information between donor and healthcare professional. Such duties are held to apply even after the death of the individual, and so it is important that similar standards of protection are maintained for information about deceased persons.

Scope

This policy applies to all collection, use, holding, sharing and disposal of person-identifiable data by or on behalf of NHSBT, irrespective of the information system used. This includes, but is not limited to, the processing of personal data as defined by GDPR. Where the term "Service" is used, this will be taken to mean the whole of NHSBT. Any exceptions will be explicitly stated.

The policy is to be observed by:

- all full time and part time employees of NHSBT, in all its functions and departments
- The Chairman, Executive and Non-Executive members of the NHSBT Board,
- The NHSBT Executive,
- contracted third parties working under the direction of NHSBT,

at any location worldwide, be that an official NHSBT site or any other location where NHSBT work is carried out...

This policy applies irrespective of the format of the information. This includes all media such as: paper, printouts, email, fax, databases, portable devices, tapes, discs, audio recordings, microfilm and CDs. It also covers verbal exchange of personal data.

Terminology

A glossary of terms used in this document and throughout Data Protection legislation and guidance is included as Appendix 2.

Policy

NHSBT must respect and protect the privacy of all individuals, be they donors, patients, employees or other supporters, with whose information it is entrusted. Gaining and maintaining the trust of stakeholders is crucial to its success in recruiting and retaining donors, and in winning and retaining customers for its products and services.

Protection of privacy is secondary to the provision of safe care to donors and patients. For this reason, full and correct details must be collected and used for identification of donors and patients, in the donation supply chain and the delivery of direct care.

Privacy is to be protected by restricting access to personal data on a 'need to know' basis. Irrespective of their compliance with duties of confidentiality, if employees can access more detail than they need for their jobs this will be regarded as a breach of policy. For any task which involves the use of personal or special category data every effort should be made to use the minimum amount of data necessary for the purpose and comply with the principles of data minimisation. Where possible, and where there would not be a clinical risk, data should be pseudonymised.

Confidentiality and Data Protection are part of a wider Information Governance agenda that seeks to ensure the confidentiality, integrity and availability of NHSBT's information assets. This is described in NHSBT's Information Governance Policy, POL266

The Caldicott Principles and the National Data Guardian (NDG)

NHSBT will promote and comply with the principles established by the committees chaired by Dame Fiona Caldicott to advise on the use and protection of patient information across the NHS, namely:

1. the purpose for using patient-identifiable data must be justified;
2. patient-identifiable data should only be used when absolutely essential
3. the minimum personal identification necessary to achieve the purpose must be used
4. access to personal confidential data should be strictly need-to-know only
5. all staff must be aware of their obligations in respect of confidential personal data
6. every use of personal data must be lawful
7. the duty to share information can be as important as the duty to protect confidentiality.

NHSBT recognises that the Caldicott Principles are consistent with yet secondary to its statutory and common law obligations, as underlined by Caldicott Principle 6

NHSBT's interpretation of Caldicott Principle 7 is that it will support the sharing of personal confidential information with third parties when the sharing is for the benefit of a patient, donor or associated third party, is necessary for and proportionate to the achievement of that benefit and is done in such a way as to balance the need for prompt availability with the risks of the method chosen.

The National Data Guardian (NDG) advises and challenges the health and care system to help ensure that citizens' confidential information is safeguarded securely and used properly, it incorporates the Caldicott Council.

Dame Fiona Caldicott was appointed as the first NDG for Health and Care by the Secretary of State for Health in November 2014. The NDG's role is to help make sure the public can trust their confidential information is securely safeguarded and make sure that it is used to support citizens' care and to achieve better outcomes from health and care services.

The NDG is guided by three main principles:

- encouraging clinicians and other members of care teams to share information to enable joined-up care, better diagnosis and treatment
- ensuring there are no surprises to the citizen about how their health and care data is being used and that they are given a choice about this

- building a dialogue with the public about how we all wish information to be used, to include a range of voices including commercial companies providing drugs and services to the NHS, researchers discovering new connections that transform treatments, and those managing the services

Compliance with the NDG recommendations and reviews is mandated through the Data Security Protection Toolkit (DSPT). IGC is responsible for managing DSPT compliance.

Information Sharing

NHSBT endorses the sharing of information with third parties where this supports the interests of patients, donors, the public or itself. Any sharing must be within the law, and supported by:

- a documented procedure for routine sharing;
- a formal contract aligned to Article 28 GDPR,
- a documented sharing agreement that includes the purposes, limits, methods and obligations of parties, or
- a record of the factors considered in deciding whether or not to share information in response to a non-standard request. that could not be covered by any of the previous bulleted items, a record of this decision must be sent to the IG team to log.

The necessary level of authority for routine sharing of information will be defined in procedure documents. Non-routine disclosures must be authorised by the Information Asset Owner. The approval of the Data Protection Officer or Caldicott Guardian or one of their delegated authorities (the Associate Medical Directors), must be obtained for non-routine disclosure of person-identifiable clinical details, for example to law enforcement agencies. If in doubt, the advice of the Information Governance Team should be sought

Lawful Basis for Processing

Under GDPR (Article 6) all information processing must have an identified legal basis to ensure that the processing is fair, lawful and justified. These legal conditions need to be identified and communicated to donors, recipients, staff, or anyone whose data NHSBT is processing.

For Special Category (formally known as Sensitive Data) you must have a lawful basis under Article 6 and Article 9 of GDPR.

The vast majority of NHSBT data processing will fall under Article 6(e)

"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"

AND

Article 9(2)(h)

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

To support choosing the correct lawful basis for data processing use the flow chart in appendix 1 or seek advice from the Data Protection Officer or Information Governance Team.

Training and Awareness

NHSBT will provide training in confidentiality and data protection within its programme of Information Governance training. Please see POL209.

Compliance and Assurance

Compliance with this policy will be checked by inclusion of audit items in the specification for national and local self-inspections. Key components will be covered by licensing authorities during their inspection visits. Additional compliance checks and audits, both internal and external, will be performed on an ad hoc basis.

Innovations, Changes and Existing Processes

All changes and developments that impact any information asset must undergo a Data Protection Impact Assessment (DPIA). This is a legal requirement in GDPR and is the responsibility of the Information Asset Owner to ensure the DPIA process is followed. This applies to all service changes and innovations, whether or not managed by the Programme Management Office. See MPD1006.

Process owners are responsible for ensuring that appropriate privacy-protecting measures are included in all procedures and work instructions, and that these measures are reviewed and updated as necessary, in consultation with the Information Asset Owner(s).

Person Identifiable Data (PID) and Pseudo-anonymisation

NHSBT will comply with the definition of PID provided in Appendix 5 of 'To Share or Not to Share?' The Information Governance Review (Caldicott 2). Care must be taken to assess the data items both singly and in combination, to establish the degree to which they may identify individuals.

At all times measures are to be applied where necessary to prevent identification and protect privacy. These may include aggregation of low-number statistics, removal of all identifiers, or partial editing of data e.g. provision of partial dates of birth, partial postcodes. Details of appropriate techniques are published by the Office for National Statistics and the Information Commissioner's Office.

Enforcement

Breach of this policy, whether knowingly or not, will be regarded as serious and will be managed under NHSBT's disciplinary policy. Applicable sanctions include dismissal, and/or referral to the criminal justice system or professional bodies.

Specific Requirements of the General Data Protection Regulation

Information and guidance about the GDPR is available from the Information Commissioner's website at ICO.org.uk.

Article 5 of the GDPR sets out seven key principles which lie at the heart of the General Data Protection regime:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Article 5(1) requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

For each information asset the lawful basis for processing data must be identified and recorded, the flow chart in Appendix 1 can be used to support a decision on which is the most appropriate basis.

(b) 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 ('purpose limitation');

When collecting data from any individual it must be established and explained to the individual the purpose of the data collection and how it is going to be used, most is covered in the NHSBT public privacy notice. Should there be a need to use the data for other purposes post collection the Information Asset owner must follow the Data Protection by Design Process and receive sign off from Information Governance and the Data Protection Officer. This is to ensure individuals are fully informed about how their data is being used and can exercise their rights should they object to the processing.

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Data collection should be kept to a minimum and relevant to support the purpose for which it is needed. If additional data would support the service but is not necessary for the purpose (for example the collection of religious beliefs would support better donor engagement) this field can be added but it must be clear to the individual the data is not mandatory and they have a clear free choice whether or not to provide the data with no impact on the care or service they receive.

(d) 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 ('accuracy');

Reasonable steps should be taken to validate the information provided and ensure it is kept up to date. This includes consistent and correct use of identifiers such as NHS number on all correspondence. Should an individual query the accuracy of the information this should be reviewed and where errors are found corrected without delay.

(e) 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 ('storage limitation');

The Information Asset Owner is responsible for ensuring all assets have set retention periods in accordance with SPN189 Records Retention specification.

(f) 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 ('integrity and confidentiality')."

Correct organisational and technical measures to protect the data must always be in place, this should be identified and put in place before the data is collected from Individuals. The Data Protection by Design process should be followed, and a Data Protection Impact Assessment (DPIA) must be completed and approved by IG and the DPO before the data is obtained.

Article 5(2) adds that:

"**The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."**

The principles lie at the heart of the GDPR. They are set out right at the start of the legislation and inform everything that follows. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of the GPDR.

Failure to comply with the principles may leave NHSBT open to substantial fines. Article 83 of the General Data Protection Regulation provides details of the possible administrative fines that could be levied against NHSBT. There are two tiers of fines. The first is up to €10 million or 2% of annual global turnover of the previous year, whichever is higher. The second is up to €20 million or 4% of annual turnover of the previous year, whichever is higher. Generally speaking, breaches of controller or processor obligations will be fined within the first tier, and breaches of data subjects' rights and freedoms will result in the higher level fine.

Individuals' Rights

GDPR imposes legal obligations on organisations under articles 12-23 of GDPR to comply with 8 fundamental individual rights. Most of these rights are not absolute and a dependent on the identified lawful basis for processing, other regulatory or statutory obligations may supersede an individual's data rights. Any request from an individual either verbal or in writing to apply their rights must be processed within 1 month, the Data Protection Officer is ultimately responsible for advising whether a right should be applied.

Data Protection Impact Assessments are the organisations main tool to ensure individual rights are not breached by new process changes.

1. **The right to be informed**

   At the point of obtaining information form an individual NHSBT must explain the purposes for processing their personal data, retention periods, and who it will be shared with.

   This data is held centrally in the NHSBT Privacy notice.

2. **The right of access**

   Individuals have the right to access their personal data, this is commonly referred to as subject access. MPD11 must be followed.

3. **The right to rectification**

   Any individual has the right to seek rectification of their records should the information contained within be incorrect. In most circumstances this right is absolute if it is agreed by both parties that the information is incorrect. Existing data should not be removed but records updated to show the change.

   A clinical record should never be retrospectively amended, even if its is agreed by all parties to contain inaccurate data, instead a note of the correct information should be made clear.

4. **The right to erasure or right to be forgotten**

   This right is not absolute; many factors should be considered when reviewing an application from an individual to apply this right. When considering this right, it is important to understand the lawful basis being relied on for processing the data, if relying on consent the individual has a much stronger case.

NHSBT has regulatory and statutory obligations for tractability and clinical record keeping which must not be compromised when applying this right. In most circumstances it will be more appropriate to apply the right to restrict processing rather than full erasure.

For the blood service a Donor retains the right to be forgotten up to the point of the session screening process. Once a DHC is received and a clinical decision has been made whether or not the individual is eligible to be a donor, the right to be forgotten no longer applies. The right to restrict processing would then apply.

For the Organ Donor register or national transplant registry either a donor or recipient can invoke their right to be forgotten up until the point where they have received clinical care.

As a rule the right to be forgotten will be restricted where specified in Art 17 (3) as follows:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims

5. The right to restrict processing

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely but will need to have the restriction in place for a certain period of time.

Individuals have the right to request you restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.

6. The right to data portability

This right only applies when processing data under explicit consent, it allows the data subject to move their data from one digital platform to another. This right will only apply in NHSBT in very limited circumstances.

7. The right to object

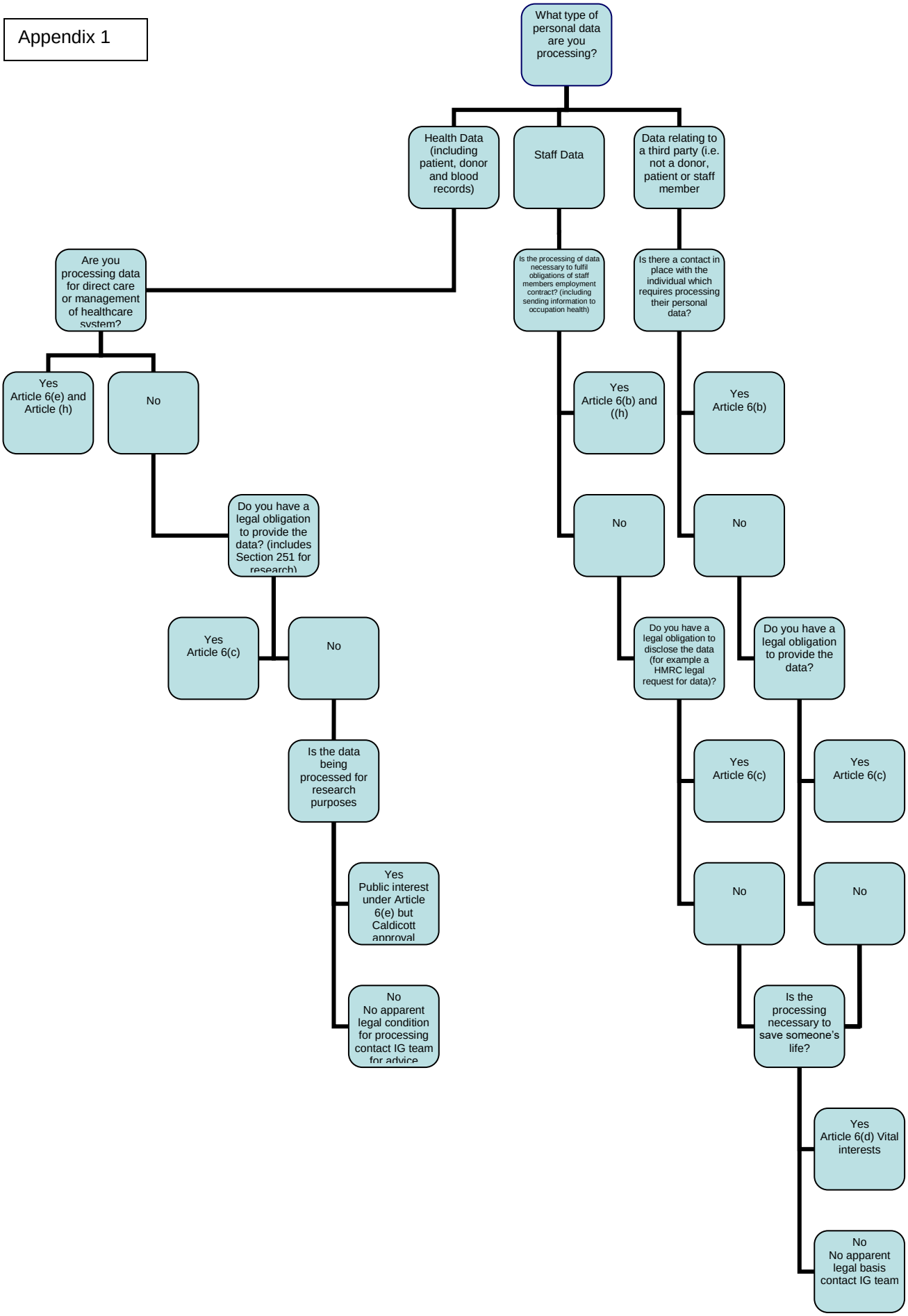
An individual can object to their data being processed where data is processed for scientific or historical research, or statistical purposes, the right to object is more restricted. When applying this right, the individual should explain their reasons for wanting to object to processing. The DPO will have to decide if the processing is in the public interest or if there are other regulatory or statutory obligations on NHSBT to retain and continue processing the data this will be decided on a case by case basis depending on the impact on the individual.

8. Rights in relation to automated decision making and profiling

An individual has the right to object to their information being used to make decisions on a purely automated basis with no human decision or intervention and to object to their data being used for the purposes of profiling unless:

- necessary for the entry into or performance of a contract; or
- authorised by UK Legislation.

Appendix 1


What type of personal data are you processing?
Health Data (including patient, donor and blood records)
Staff Data
Data relating to a third party (i.e. not a donor, patient or staff member
Are you processing data for direct care or management of healthcare system?
Is the processing of data necessary to fulfil obligations of staff members employment contract? (including sending information to occupation health)
Is there a contact in place with the individual which requires processing their personal data?
Yes Article 6(e) and Article (h)
No
Yes Article 6(b) and ((h)
Yes Article 6(b)
Do you have a legal obligation to provide the data? (includes Section 251 for research)
No
No
Yes Article 6(c)
No
Do you have a legal obligation to disclose the data (for example a HMRC legal request for data)?
Do you have a legal obligation to provide the data?
Is the data being processed for research purposes
Yes Article 6(c)
Yes Article 6(c)
Yes Public interest under Article 6(e) but Caldicott approval
No
No
No No apparent legal condition for processing contact IG team for advice
Is the processing necessary to save someone's life?
Yes Article 6(d) Vital interests
No No apparent legal basis contact IG team

APPENDIX 2

Glossary of Terms

GDPR - The **General Data Protection Regulation** (EU) 2016/679

Individual's – Any living person whose data is being processed by NHSBT, this can include but is not limited to; Donors, Recipients, staff members, third party contractors.

Information Commissioner's Office (ICO) – The body that oversees the implementation of and compliance with the GDPR, Data Protection Act 2018, the Freedom of Information Act 2000 and the Environmental Information Regulations 2005). See www.ICO.org.uk.

Data Controller – The legal body (in this case the NHSBT) which determines the purposes and manner of processing personal data and is legally responsible for the proper management of those personal data.

Data Processor – An individual or company which undertakes processing of personal data on behalf of a Data Controller.

Personal Data – Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. Personal data may exist in electronic or hard copy format, including databases, emails, paper files, audio tapes, CCTV tapes, etc.

Processing – Doing almost anything with personal data, including collecting, using, storing, viewing, analysing, disclosing, updating, amending, archiving or destroying it.

Data Subjects – The individuals that the information or data is about.

Notification – The system by which Data Controllers inform the ICO of the purposes for which they process personal data. This information is published as a Register of Data Controllers and accessible online at www.ico.org.uk.

Data Protection Principles – The eight principles of good information handling which form the basis of the requirements of the Act

Caldicott Principles: The seven principles of handling and sharing patient/donor information across the NHS established by the committees chaired by Dame Fiona Caldicott

Subject Access Request – The process by which Data Subjects may request disclosure of their information held by a Data Controller.

Third Party – Anyone other than the Data Subject, the Data Controller and any Data Processor.

Pseudonymisation and Anonymisation – Pseudonymisation and Anonymisation are different in one key aspect. Anonymisation irreversibly destroys any way of identifying the data subject. Pseudonymisation substitutes the identity of the data subject in such a way that additional information is required to re-identify the data subject.

Data Minimisation - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.