

DATA SHARING AGREEMENT

Between

The Infected Blood Compensation Authority

And

Infected Blood Support Schemes (EIBSS, SIBSS, WIBSS, NIIBSS)

Relating to

Infected Blood Compensation Delivery

This Data Sharing Agreement is made as of the dates set out in the 'Signatures' section at the end of this document.

Between

(1) The Infected Blood Compensation Authority ("IBCA"), of Floor 3, Block 2, Benton Park View, Newcastle-upon-Tyne, NE98 1ZZ

(2) **Infected Blood Support Scheme (England Infected Blood Support Scheme (EIBSS), Scottish Infected Blood Support Scheme (SIBSS), Wales Infected Blood Support Scheme (WIBSS), Northern Ireland Blood Support Scheme (NIIBSS))** together referred to as "the Schemes"

Who will be collectively referred to as "the Parties".

Purpose of this Agreement

The purpose of this agreement is to address the sharing of Personal Data (as listed in Annex 1) between the Parties.

It sets out the categories of Personal Data that will be shared and the purposes for sharing. It also documents the Controller responsibilities of the Parties regarding the processing of Personal Data shared under this Agreement and the way data protection compliance will be ensured in practice.

Definitions

Unless otherwise stated, the words and expressions listed below shall have the following meanings:

UK GDPR: means the United Kingdom's retained version of the General Data Protection Regulation ((EU) 2016/679) as defined in section 3(10) (and as supplemented by section 205(4)) of the DPA 2018. **DPA 2018:** Data Protection Act 2018.

Data Protection Legislation: (i) the UK GDPR as amended from time to time (ii) the DPA 2018 as amended from time to time (iii) all applicable Law about the processing of personal data and privacy as amended from time to time, including "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law;", where applicable **Controller, Processor, Processing, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer, Data Protection Impact Assessment:** take the meaning given in the UK GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the DPA 2018 applies, the meaning in that part if different.

Data Protection Principles: means the principles set out in Article 5 of the UK GDPR.

Data Subject Rights: means those rights set out in Chapter III of the UK GDPR.

Subject Access Request: means the rights of data subjects set out in Article 15 of the UK GDPR.

Law: means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, , regulation, order, regulatory policy, mandatory

guidance or code of practice, judgement of a relevant court of law, or directives or requirements with which the Parties are bound to comply.

Personnel: means all directors, officers, employees, agents, consultants and contractors engaged in the Processing of Personal Data.

DPO: Data Protection Officer.

DPIA: Data Protection Impact Assessment.

Protective Measures: means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures.

Roles

The Parties acknowledge that for the purposes of the Data Protection Legislation, the Parties are Independent Data Controllers for sets of Personal Data and Special Category Data processed and shared pursuant to the agreement.

The Parties agree that the scope of this Agreement applies as far as the data items stated in Annex 1.

The Parties further agree that they will;

- Carry out any required Data Protection Impact Assessment for the processing of the data.
- Ensure staff have appropriate security clearance to process the personal data as part of this Agreement.
- Comply with the data protection principles, and with all relevant data protection legislation.
- Follow their departmental Security Guidance to ensure that the necessary measures are taken to protect personal data.

Agreed Purposes

It is agreed that the data items stated in Annex 1 shall only be processed by the Parties for the following purposes:

IBCA

- Obtaining Data from the Schemes in order to design the IBCA compensation Scheme to support applicants who wish to apply.
- To establish eligibility for compensation.
- Applicants will not need to supply information already held by the Schemes, in accordance with the 'Tell Us Once' government principle.

The Schemes

- The Schemes have access to data held by The Skipton Fund in order to administer the Infected Blood Interim Compensation Payment Scheme (IBICPS).

Furthermore the Parties agree to maintain all security measures and processes as stated in this Agreement whilst retaining the Personal Data.

The purpose of the data sharing initiative

Obtaining Data from the Schemes in order to design the IBCA Compensation Scheme to support applicants who wish to apply and to establish eligibility for compensation.

Why is the sharing of the data necessary?

The sharing of the data is necessary in order to:

- design a compensation scheme around actual user needs, and subsequently to match this data to individuals so that we can consider it alongside their applications for compensation, and
- enable the Schemes to administer the estates portion of the IBICPS.
- enable the Schemes to administer the Infected Blood Payments Scheme

By sharing the data IBCA aims to achieve:

- the support of applications for the compensation scheme administered by IBCA, from infected and affected applicants.
- Data shared by the Schemes to IBCA is to be used for this purpose.

By sharing the data the Schemes aim to achieve:

- The Schemes will have access to the digital platform which contains The Skipton Fund Data in order to deliver the estates portion of the IBICPS.s.
- IBCA are to assign licences to the 4 Schemes within the UK so that they can access this data to facilitate the delivery of estate payments under Section 56 Victims and Prisoners Act 2024. The Schemes will have access to the digital platform which contains The Skipton Fund Data in order to support the administration of the Infected Blood Payments Scheme. The data shared by IBCA to the Schemes will be used for this purpose.

The benefits for individuals or to society more widely are:

- Effective design of the compensation scheme will support applicants who wish to apply.
- IBCA having access to this data will assist applicants in establishing their eligibility for compensation.
- Having access to this data will avoid the need for applicants to supply the same information again to IBCA, in accordance with the 'Tell Us Once' government principle.
- This will enable the Schemes to have access to Skipton Fund Data to streamline payment to the estates Blood Interim Compensation Payment Scheme.
- This will enable the Schemes to have access to Skipton Fund Data to streamline payment to the Infected Blood Payments Scheme.

What is the lawful basis for sharing?

All parties will rely on Article 6 1(e) UK GDPR: 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 data controller. In this case that is discharging the function of the Infected Blood Compensation Authority as set out by the Victims and Prisoners Act 2024, in particular, part 3 sections 48 to 57 infected blood compensation <https://www.legislation.gov.uk/ukpga/2024/21/part/3>, and associated Regulations.

Special Category Data:

Article 9 2(g) UK GDPR “Substantial Public Interest” is the basis for sharing Special Category Data.

The Schedule 1 Part 2 Substantial Public Interest Condition is paragraph 6 Statutory and government purposes:

6(1) This condition is met if the processing—

- (a) is necessary for a purpose listed in sub-paragraph (2), and
- (b) is necessary for reasons of substantial public interest.

(2) Those purposes are—

- (a) the exercise of a function conferred on a person by an enactment or rule of law;
- (b) the exercise of a function of the Crown, a Minister of the Crown or a government department.

Criminal Offence Data:

Insofar as any criminal offence data appears as part of the relevant datasets, the lawful basis for processing this will be, pursuant to Article 10 of the UK GDPR, as above - Paragraph 6 of Schedule 1 - Statutory and government purposes.

Legal Gateway - Victims and Prisoners Act 2024

Section 53(2) - The IBCA may by notice in writing require a person to provide information to the IBCA for the purposes of any matter connected with the administration of the infected blood compensation scheme.

IBCA will be relying on this provision to request information from the Schemes, and the Schemes will be relying on this to provide it to IBCA.

Section 53(1) - The IBCA may provide information to another person for the purposes of any matter connected with the administration of the infected blood compensation scheme.

IBCA will be relying on this provision to provide data access to the Schemes.

Lawful, fair and transparent processing

Each Party shall ensure that it processes the Personal Data fairly and lawfully in accordance with Data Protection Legislation and the principles set out under Article 5 of the UK GDPR.

Each Party shall ensure that the Personal Data is:

- (i) Adequate, relevant and limited to what is necessary in relation to the purposes for which the personal data is processed under this Agreement; and
- (ii) Accurate and, where necessary, up to date; having taken every reasonable step to ensure that any inaccurate personal data (having regard to the purposes for which the personal data is processed under this Agreement) has been erased or rectified.

Each party shall, in respect of the Project Personal Data, ensure they provide clear and sufficient information to the data subjects, in accordance with the Data Protection Legislation.

Each party will be responsible for their own privacy notices and confirms that one will be available as at the time data is shared, which covers this processing.

Access and individual rights

Once each party receives (and accordingly holds) the data being shared, they accept that they will be responsible for responding to the following in relation to the processing of the data undertaken by them, involving the data provided under this Agreement:

- (a) Data Subject Requests (or purported Data Subject Request);
- (b) requests to rectify, block or erase any Personal Data;
- (c) any other requests, complaints or communications relating to either Party's obligations under the Data Protection Legislation;
- (d) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
- (e) requests from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
- (f) any Data Loss Event.

When responding to Data Subject Access Requests, which would include the shared data, they will notify IBCA of the request and obtain confirmation that such data can be released. IBCA commits that they will provide the confirmation within the necessary statutory timescale for Data Subject Access Requests.

Contact with the IBCA Data Privacy and Compliance Team to be made via email to ibca.datagov@cabinetoffice.gov.uk

Data Security

The Parties acknowledge that as Independent Data Controllers they shall, in relation to any Personal Data processed in connection with this Agreement:

- (a) ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, having taken account of the:
- (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;

Additionally, all staff that will process the data on behalf of the Parties, will have received appropriate training to ensure secure and compliant processing.

The Parties agree that any data security measures notified to the other Party prior to the provision of the agreed data will be maintained whilst the data is subject to processing.

Data Breaches.

The Recipient as an Individual Data Controller shall, in relation to any Personal Data supplied under this Agreement will ensure that where a breach occurs, they will be required to:

- Advise the other Party's Data Protection Officer of the breach
- Undertake a full investigation to identify the cause and the remedial action necessary to prevent re-occurrence.
- Identify if the incident should be notified to the Information Commissioner's Office (ICO) and if so, advise the other party's Data Protection Officer prior to notifying the ICO.
- issue the other Party's Data Protection Officer with ongoing reports and subsequent updates regarding the incident until the necessary process has been finalised.
- implement any measures necessary to restore the security of compromised Personal Data.

Contact with the IBCA Data Privacy and Compliance Team is to be made via email to ibca.datagov@cabinetoffice.gov.uk

Sharing Effectiveness

This Agreement will remain valid until 31 March 2026, subject to annual review . During this time the effectiveness and need for the sharing will be reviewed periodically. If it is identified that the data being shared is not achieving the benefits stated, the data items will be reviewed to identify if changes are needed. If this is necessary Annex 1 will be updated, subject to the Agreement being signed off by relevant controllers again.

If amendments to the data items cannot produce the stated benefits, the Agreement will be exited by both parties and no further data will be shared by the Parties, in accordance with the 'exiting this agreement' section of this agreement. In the event of an early exit or the conclusion of this agreement, no further data will be exchanged between the Parties, with information already held being limited to only being able to use it for purposes stated in this agreement.

Data Accuracy

It is the responsibility of the Data Controller sharing data as the providing Party of the data to ensure the data that is shared is accurate and up to date. Note however that data provided to the Schemes to assist with estate payment delivery has been previously retained by another Data Controller. IBCA has acquired this in an 'As-Is' state at the time of transfer, and it is provided as such.

Each of the Parties shall advise the other if any of the data shared requires amendment or if an individual is exercising their data protection rights.

Each Party is required to advise the other as soon as possible if it becomes aware of any changes to the shared data that need to be made.

Data retention and deletionThe Parties shall not retain or process Personal Data for longer than is necessary to carry out the Agreed Purposes. Notwithstanding, the Parties shall continue to retain Personal Data in accordance with any statutory or professional retention periods applicable in their respective organisation.

IBCA are proposing to keep documents for 8 years from determination to match the expected window of the scheme, with summary data to be retained for longer due to exempted limitation claims, in order to prevent duplicate applications as a fraud prevention measure.

Determination in this context means final decision, as in following an offer of compensation being accepted, or all reviews/appeals exhausted with respect to any contested/refused application.

Schemes are to retain personal data until such time as this is transferred to IBCA

Technical and organisational security arrangements

The data will be securely provided by IBCA to the Schemes by the following means:

- [REDACTED]
- [REDACTED]

The data will be securely provided by the Schemes to IBCA by the following means:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

The frequency of the data provision to IBCA from the Schemes is agreed to be:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

The frequency of the data provision to the Schemes from IBCA is agreed to be:

[REDACTED]
[REDACTED]

The Schemes agree to securely store the data shared as follows:

Where data is downloaded from [REDACTED], Schemes confirm they have a fully documented retention policy and Retention Schedule and Records Management policies in place which apply to this data, as well as appropriate access controls, security policies and safeguards.

IBCA agrees to securely store the data received from the Schemes as follows:

In [REDACTED] with appropriate role-based access controls and security policies.

Where any data will be hosted outside the UK due to the [REDACTED] [REDACTED] this is covered by either applicable adequacy decisions (in the case of e.g. EU data centres), or a UK International Data Transfer Agreement for other third countries.

IBCA uses [REDACTED] supplied by an agreement with [REDACTED] [REDACTED] supplier is [REDACTED] and any data transferred to [REDACTED] is covered by a UK adequacy decision.

Technologically, [REDACTED] stores production and back up data in a distributed away across a range of international data centres using its [REDACTED].

Onward transfer of data from [REDACTED] to international data centres is made lawful (under EU GDPR) by virtue of the EU-US Data Privacy Framework (a form of adequacy agreement), and to other international territories by virtue of processor-to-processor Standard Contractual Clauses approved by the European Commission.

Dispute resolution

If either of the Parties has any issues, concerns or complaints about this agreement it shall notify the other and they shall, acting in good faith, seek to resolve the issue by negotiations between themselves.

All issues, concerns or complaints should in the first instance be raised with the individuals responsible for the monitoring of this agreement as stated in Annex 2.

Exit from the Agreement

In the event of an early exit or the conclusion of this agreement, no further data will be exchanged between the parties, with information already held being limited to only being able to use it for purposes stated in this agreement. Early exit from this agreement can be made by giving all Parties one months notice.

This Agreement shall be terminated on 31 March 2026, unless a formal review is conducted and both controllers mutually agree to extend the terms of the agreement.

SIGNATURES

The signatories agree that the procedures laid down in this Agreement provide an acceptable framework for the sharing of information between themselves, and that it is in a manner compliant with their statutory and professional responsibilities.

By signing this agreement, the signatories undertake to accept responsibility for implementation of the terms of this Agreement within their own organisations.

Signatories must also ensure that they comply with all relevant legislation.

Signed by:

Department Name	IBCA
Signed on behalf of Department Business Unit	
Print Name (Block Capitals)	
Date	15/10/24

Department	Department of Health NI
Signed on behalf of Department Business Unit	
Print Name (Block Capitals)	
Date	17/10/2024

Department	Regional Business Services Organisation (NI)
------------	--

Signed on behalf of Department Business Unit	
Print Name (Block Capitals)	
Date	18-10-2024

Department	WIBSS
Signed on behalf of Department Business Unit	
Print Name (Block Capitals)	
Date	15/10/2024

Department	SIBSS
Signed on behalf of Department Business Unit	
Print Name (Block Capitals)	
Date	16/10/2024

Department	EIBSS
Signed on behalf of Department Business Unit	[REDACTED]
Print Name (Block Capitals)	[REDACTED]
Date	16/10/2024

Annex 1

Data Items to be shared

Data Items	To be used for (as applicable):
<i>All relevant data items held by the Skipton Fund and the Schemes, as including but not limited to:</i> <i>bank account, personal ID documentation, probate documentation and medical information.</i> <i>will also include personal details of family members such as dependent children and next of kin.</i> <i>Applicant ID</i> <i>Applicant Name</i> <i>Surname</i> <i>NI Number</i> <i>Category</i> <i>Haemophilia Centre</i>	<i>Service Design of the IBCA compensation scheme</i> <i>Subsequent assessment of eligibility for compensation, where such an application is received.</i> <i>Determination and delivery of IBICPS estate payments.</i> <i>Determination and delivery of Infected Blood Support Scheme Payments.</i>

<i>3rd Party</i>	
<i>Region</i>	
<i>Date Application Received</i>	
<i>Status</i>	
<i>Doctor Name</i>	
<i>Date Of Appeal</i>	
<i>Ref with suffix</i>	
<i>Ref</i>	
<i>suffix</i>	
<i>surname</i>	
<i>first names</i>	
<i>middle name</i>	
<i>date of birth</i>	
<i>date of death</i>	
<i>Country of infection</i>	
<i>title</i>	
<i>second name</i>	
<i>notes/If Family Member (FM) name of original PB</i>	
<i>Vendor ID</i>	
<i>Payment Date</i>	
<i>Receipt Of Payment</i>	
<i>PPC</i>	
<i>Top Up Payments</i>	

<i>Regular Payments</i> <i>Vendor Address - Contact</i> <i>Type of applicant</i> <i>personal details of family members such as dependent children and next of kin.</i> <i>(Per [REDACTED]) "we do not know exactly what personal data is contained in each of the files as this very much depends on what the individuals disclosed in relation to their cases."</i>	
--	--

Annex 2

Contacts Relevant to this Data Sharing Agreement

The individuals that have arranged this agreement are:

Role/Department	Name	Email

Commented [1]: Scheme contacts

IBCA Data Governance		Ibca.datagov@cabinetoffice.gov.uk
EIBSS		
NIIBSS		
SIBSS		
WIBSS		

The individuals responsible for the monitoring of this agreement are:

Commented [2]: Scheme Info Gov managers

Role/Department	Name	Email
IBCA DPO		dpo@cabinetoffice.gov.uk
NHSBSA DPO		dataprotection@nhsbsa.nhs.uk

