

Date 30/07/2025
Your Ref
Our Ref 10289

Enquiries to Richard Mutch
Extension 35687
Direct Line 0131 465 5687
loth.freedomofinformation@nhs.scot
richard.mutch@nhs.scot

Dear

FREEDOM OF INFORMATION – MD CONSENTS

I write in response to your request for information in relation to MD Consents.

Question:

- Under the Freedom of Information (Scotland) Act 2002, I request the following information regarding the digital consent platform “MD Consents” (<https://mdconsents.com/>) currently used by NHS Lothian:
 - Contract details
 - Dates of commencement and expiry (including any extensions) of any contract(s) between NHS Lothian and MD Consents Ltd (or related entities).
 - Contract duration and renewal terms.
 - Total amounts paid (or projected to be paid) under these agreements to date.

Answer:

Initial contract
Effective date - 02.12.2020
Term - Until fifth anniversary of effective date
Annual charge - £23,408

Contract update
Effective date - 02.12.2023
Term - Until fifth anniversary of effective date
Annual charge - £34,867

Question:

- Data retention and disposal
 - Copies of the retention schedule/policy applicable to data collected via MD Consents.
 - Retention durations for specific data types (e.g. consent forms, audit logs).
 - Procedures for secure deletion or archiving once retention periods have lapsed.

Headquarters
Mainpoint
102 West Port
Edinburgh EH3 9DN

Chair Professor John Connaghan CBE
Chief Executive Professor Caroline Hiscox
Lothian NHS Board is the common name of Lothian Health Board



Answer:

| | |
|----|--|
| a. | Please see attached document 04 Data Processes & Flows for details of the retention schedule/policy applicable to data collected via MD Consents |
| b. | See attached document 04 Data Processes & Flows for details for details of the retention durations for data |
| c. | See attached document 04 Data Processes & Flows for details of the procedures for secure deletion and archiving |

Question:

3. Information governance / risk assessments

- a. Copies of any Data Protection Impact Assessments (DPIAs) or equivalent evaluations performed in relation to MD Consents.
- b. Records of any cyber/security risk assessments, vulnerability testing, or data-sharing reviews undertaken.
- c. Any formal Caldicott Guardian sign-off or legal/IGD approvals related to deploying MD Consents.

Answer:

| | |
|----|---|
| a. | The DPIA for IDEAS includes the integration of the existing, nationally approved Fertility Consents platform. |
| b. | IT Security documentation is not subject to disclosure. As detailed in the DPIA, the project is subject to review in March 2026. |
| c. | The DPIA is reviewed and approved by an Information Governance Project Manager on behalf of NHS Lothian. The Data Processing Agreement is signed by the NHS Lothian Caldicott Guardian. |

NHS Lothian has a policy of not releasing the names and details of staff below a senior level, this information has been redacted under Section 38(1)(b) of the Freedom of Information (Scotland) Act 2002 – personal information.

Security documents have been redacted as release would be likely to prejudice substantially the Board’s ability to exercise a number of its purposes, but particularly those described under FOISA section 30(c) i.e., be likely to prejudice substantially effective conduct of public affairs. For this reason, we believe that the exemption under FOISA, section 30(c) applies to the information requested.

We acknowledge that any exemption applying under section 30 is also subject to the public interest test. We have therefore applied the public interest test and subsequently determined that, in the context of this specific case, the public interest in maintaining the exemption outweighs that in disclosure of the information.”

I hope the information provided helps with your request.



If you are unhappy with our response to your request, you do have the right to request us to review it. Your request should be made within 40 working days of receipt of this letter, and we will reply within 20 working days of receipt. If our decision is unchanged following a review and you remain dissatisfied with this, you then have the right to make a formal complaint to the Scottish Information Commissioner within 6 months of receipt of our review response. You can do this by using the Scottish Information Commissioner's Office online appeals service at www.itspublicknowledge.info/Appeal. If you remain dissatisfied with the Commissioner's response you then have the option to appeal to the Court of Session on a point of law.

If you require a review of our decision to be carried out, please write to the FOI Reviewer at the email address at the head of this letter. The review will be undertaken by a Reviewer who was not involved in the original decision-making process.

FOI responses (subject to redaction of personal information) may appear on NHS Lothian's Freedom of Information website at: <https://org.nhsllothian.scot/FOI/Pages/default.aspx>

Yours sincerely

ALISON MACDONALD
Executive Director, Nursing
Cc: Chief Executive
Enc.



DATA PROCESSING AGREEMENT

BETWEEN

NHS Lothian

AND

MELLOWOOD MEDICAL INC

Date: May 2024

Review date: May 2026

INDEX

1 DEFINITIONS 3

2 CONTROLLER/PROCESSOR AND PERSONAL DATA 6

3 COMPLIANCE WITH DATA PROTECTION LEGISLATION 7

4 PROCESSING INSTRUCTIONS 7

5 ASSISTANCE TO THE BOARD 7

6 TECHNICAL AND ORGANISATIONAL MEASURES 8

7 CONTRACTOR PERSONNEL 8

8 INTERNATIONAL TRANSFERS OF PERSONAL DATA 9

9 NOTIFICATIONS REQUIRED TO BE GIVEN BY THE CONTRACTOR TO THE BOARD 9

10 RECORDS 10

11 USE OF SUB-PROCESSORS 10

12 AUDIT RIGHT 11

13 DELETION OR RETURN OF PERSONAL DATA 11

14 LIABILITY 12

15 GENERAL 12

SCHEDULE 15

DATA PROCESSING AGREEMENT

between

NHS Lothian

a statutory body constituted pursuant to the National Health Service (Scotland) Act 1978 (as amended) and having its headquarters at **Waverley Gate, 2-4 Waterloo Place, Edinburgh, EH1 3EG** (the "Board")

and

Mellowood Medical Inc

a company registered under the Companies Acts (Registration No. **[864908645TR0002 (Canada)]** and having its registered office at **[45 Mellowood Drive, Suite1B, Toronto ON Canada M2L2E4]** (the "Contractor")

YES MIMI

Commented [WD1]: Can this be completed

WHEREAS:

- A. The Board has engaged the Contractor to provide the Services (as defined below and the Contractor will Process Personal Data (all as defined below) in the provision of the Services.
- B. In order to comply with the Data Protection Legislation (as defined below), the Parties require to enter into this Agreement to regulate the Processing of the Personal Data and related matters.

NOW IT IS HEREBY AGREED as follows:-

1 DEFINITIONS AND INTERPRETATION

1.1 In this Agreement, the following expressions shall have the following meanings:

- "Agreement"** means this data processing agreement, including the Schedule;
- "Appropriate Safeguards"** means a legally compliant mechanism(s) for the transfer of Personal Data to a country outside the EEA in respect of which no adequacy decision has been made by the European Commission, as such mechanism(s) may be permitted under the Data Protection Legislation from time to time;

| | |
|--|--|
| "Business Day" | means Monday to Friday excluding public holidays as observed by the Bank of Scotland in Edinburgh; |
| "Contractor Personnel" | means any and all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any Sub-processor engaged in the performance of the obligations imposed on the Contractor pursuant to or under this Agreement, including but not limited to the performance of the Services; |
| "Controller" | shall have the meaning given in the GDPR; |
| "Data Loss Event" | means any event, including but not limited to any Personal Data Breach, that results, or may result, in unauthorised access to Personal Data held by the Contractor or any Sub-processor under or in connection with this Agreement and/or actual or potential loss and/or destruction and/or corruption of Personal Data in breach of this Agreement; |
| "Data Protection Impact Assessment" | means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data; |
| "Data Protection Legislation" | means (i) the GDPR and any applicable national implementing Laws as amended from time to time; (ii) the DPA 2018 to the extent that it relates to the Processing of Personal Data and privacy; and (iii) any other Law in force from time to time with regards to the Processing of Personal Data and privacy, which may apply to either Party in respect of its activities under this Agreement ; |
| "Data Protection Officer" | shall have the meaning given in the GDPR; |
| "Data Subject" | shall have the meaning given in the GDPR; |
| "Data Subject Access Request" | means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data; |
| "Direct Losses" | means all damage, losses, indebtedness, claims, actions, cash, expenses (including the cost of legal or professional services) legal costs, proceedings, demands and charges whether arising under statute, contract or at common law excluding Indirect Losses; |
| "DPA 2018" | means the Data Protection Act 2018; |
| "DP Losses" | means all liabilities and amounts, including all: <ul style="list-style-type: none"> a) Direct Losses; b) costs and expenses relating to reconstitution and/or correction of the Personal Data and any and all records comprising the same; and |

- c) to the extent permitted by Applicable Law:
 - (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; and
 - (ii) compensation to a Data Subject ordered by a Supervisory Authority;

| | |
|--|---|
| "Effective Date" | means the last date of execution of this Agreement |
| "EEA" | means the European Economic Area; |
| "GDPR" | means the General Data Protection Regulation (UK) |
| "Indirect Losses" | means loss of profits, loss of business, loss of business opportunity, loss of goodwill or any consequential loss or indirect loss of any nature; |
| "Information Commissioner's Office" | means the United Kingdom's Supervisory Authority; |
| "Law" | means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Board and/or the Contractor is bound to comply; |
| "Minimum Requirements" | means those requirements identified as such in Schedule; |
| "Party" | means a Party to this Agreement; |
| "Personal Data" | shall have the meaning given in the GDPR; |
| "Personal Data Breach" | shall have the meaning given in the GDPR; |
| "Processing" | shall have the meaning given in the GDPR and the terms "Process" and "Processed" shall be construed accordingly; |
| "Processor" | shall have the meaning given in the GDPR; |
| "Protective Measures" | means appropriate technical and organisational measures which must include the Minimum Requirements and may also include, without limitation: pseudonymising and encrypting Personal Data; ensuring confidentiality, integrity, availability and resilience of systems and services used by the Contractor and, where relevant, by any Sub-processor in connection with the performance of the obligations imposed on the Contractor pursuant to or under this Agreement, including but not limited to the performance of |

the 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 technical and organisational measures adopted from time to time by the Contractor and, where relevant, by any Sub-processor;

- "Representative"** shall have the meaning given in the GDPR;
- "Schedule"** means the schedule annexed to and forming part of this Agreement;
- "Services"** **the meaning given in the Services Agreement.**
- "Services Agreement"** **means the agreement between the Contractor and the Board**
- "Sub-processor"** means any third party appointed to process Personal Data on behalf of the Contractor in connection with this Agreement;
- "Supervisory Authority"** shall have the meaning given in the GDPR; and
- "Term"** means the period from the Effective Date until the Agreement is terminated in accordance with its terms.

- 1.2 In this Agreement unless the context otherwise requires it:-
- 1.2.1 the Clause headings are for reference only and shall not affect the construction or interpretation of this Agreement and references to the Schedule, sub-clauses and clauses are to the Schedule, sub-clauses and clauses in this Agreement;
 - 1.2.2 the singular includes the plural and vice versa;
 - 1.2.3 references to gender include references to all genders;
 - 1.2.4 reference to a "person" includes any individual, partnership, firm, company, corporation, joint venture, trust, association, organisation or other entity, in each case whether or not having a separate legal personality;
 - 1.2.5 references to statutes, any statutory instrument, regulation or order shall be construed as a reference to such statute, statutory instrument, regulation or order as amended, consolidated, replaced or re-enacted from time to time; and
 - 1.2.6 the words "include" or "including" are to be construed as meaning without limitation.

2 CONTROLLER/PROCESSOR AND PERSONAL DATA

- 2.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Board is the Controller and the Contractor is the Processor.
- 2.2 For the avoidance of doubt, references in this Agreement to the term "Personal Data" shall only apply to Personal Data Processed in the course of the performance of the

obligations imposed on the Contractor pursuant to or under this Agreement, including but not limited to the performance of the Services.

3 COMPLIANCE WITH DATA PROTECTION LEGISLATION

- 3.1 The Contractor warrants that it will, and will procure that any and all Sub-processors will, at all times throughout the Term, Process Personal Data in compliance with the Data Protection Legislation.

4 PROCESSING INSTRUCTIONS

- 4.1 The only Processing that the Contractor is authorised to undertake in connection with the performance of the obligations imposed on the Contractor pursuant to or under this Agreement, including but not limited to the performance of the Services is listed in the Schedule, as the same may be amended from time to time by written agreement between the Parties. The Contractor warrants that it will, and will procure that any and all Sub-processors will, at all times throughout the Term, only Process the Personal Data for the purposes of the performance of the obligations imposed on the Contractor pursuant to or under this Agreement, including but not limited to the performance of the Services.
- 4.2 The Contractor shall promptly comply with any written request from the Board requiring the Contractor to amend, transfer or delete the Personal Data.
- 4.3 The Contractor shall notify the Board immediately if it considers that any of the Board's instructions infringe the Data Protection Legislation and will provide the Board with a written explanation of the reasons why it considers any of the Board's instructions to be so infringing.

5 ASSISTANCE TO THE BOARD

- 5.1 The Contractor shall, as part of the Services and at no additional cost or expense to the Board, provide all reasonable assistance to the Board in ensuring compliance with the Board's obligations under the Data Protection Legislation in relation to:
- 5.1.1 ensuring the security of the Personal Data;
 - 5.1.2 any notifications, communications and remedial action that may be required to be made or taken following any Data Loss Event, including notifications to the relevant Supervisory Authority following a Data Loss Event and communications to affected or potentially affected Data Subjects;
 - 5.1.3 responding to Data Subject Access Requests within the timescale set out in the Data Protection Legislation;
 - 5.1.4 any request from a Supervisory Authority or any consultation by the Board with a Supervisory Authority, to the extent that such request or consultation relates to or involves the Processing undertaken by the Contractor and/or any Sub-processor under or in connection with this Agreement;
 - 5.1.5 the preparation of any Data Protection Impact Assessment prior to commencing any new Processing that has been agreed between the Parties pursuant to Clause 4.1. Such assistance may, at the discretion of the Board, include:
 - 5.1.5.1 a systematic description of the envisaged Processing operations and the purpose of the Processing;

- 5.1.5.2 an assessment of the necessity and proportionality of the Processing operations in relation to the performance of the obligations imposed on the Contractor pursuant to or under this Agreement, including but not limited to the performance of the Services;
- 5.1.5.3 an assessment of the risks to the rights and freedoms of Data Subjects; and
- 5.1.5.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

5.2 At any time throughout the Term, or following the date of termination, at the request of the Board, the Contractor shall provide to the Board a copy of all Personal Data held by the Contractor in the format and on the media reasonably specified by the Board. If the Contractor fails to provide the Board with a copy of such requested Personal Data the Board may, without limiting its other rights or remedies, enter the Contractor's premises and take a copy of such Personal Data.

6 TECHNICAL AND ORGANISATIONAL MEASURES

6.1 The Contractor shall:

- 6.1.1 Process the Personal Data only in accordance with the Schedule, unless the Contractor is required to do otherwise by Law, in which case the provisions of Clause 4.3 shall apply;
- 6.1.2 ensure that it has in place Protective Measures, which the Contractor shall maintain throughout the Term at its cost and expense, and which are appropriate to protect against a Data Loss Event, having taken account of:
 - 6.1.2.1 the nature of the Personal Data to be protected;
 - 6.1.2.2 the harm that might result from a Data Loss Event;
 - 6.1.2.3 the state of technological development; and
 - 6.1.2.4 the cost of implementing any measures

7 CONTRACTOR PERSONNEL

- 7.1 The Contractor shall ensure that it takes all reasonable steps to ensure the reliability and integrity of any Contractor Personnel who have access to the Personal Data and ensure that they:
 - 7.1.1 are aware of and comply with the Contractor's duties under this Agreement, in particular those obligations set out in this Agreement;
 - 7.1.2 are subject to appropriate confidentiality undertakings with the Contractor or any Sub-processor, as the case may be, which confidentiality undertakings require the Contractor Personnel to keep the Personal Data confidential and to only Process the Personal Data for the purposes of the performance of the obligations imposed on the Contractor pursuant to or under this Agreement, including but not limited to the performance of the Services;
 - 7.1.3 are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Board or as otherwise permitted by this Agreement; and

7.1.4 have undergone adequate training in the use, care, protection and handling of Personal Data and on the Data Protection Legislation insofar as it relates to Processing.

8 INTERNATIONAL TRANSFERS OF PERSONAL DATA

- 8.1 The Contractor shall not transfer Personal Data outside of the United Kingdom without the prior written consent of the Board.
- 8.2 Where the Contractor wishes to transfer Personal Data to a country within the EEA, the Board's consent shall not be unreasonably withheld or delayed.
- 8.3 If the Board gives its written consent to a transfer of Personal Data outside of the EEA, the Contractor shall ensure that:
- 8.3.1 the Contractor has Appropriate Safeguards in place in respect of such transfer and, where practicable, the particular Appropriate Safeguards to be used by the Contractor for such transfer shall be subject to the Board's prior written approval, which approval shall not be unreasonably withheld or delayed;
 - 8.3.2 the transfer and any Processing of Personal Data following such transfer complies at all times with Clause 4.1; and
 - 8.3.3 the transfer otherwise complies with Data Protection Legislation.

9 NOTIFICATIONS REQUIRED TO BE GIVEN BY THE CONTRACTOR TO THE BOARD

- 9.1 The Contractor shall, at its own cost and expense, notify the Board immediately (and within three (3) Business Days of receipt of the relevant communication at the latest) if it
- 9.1.1 receives a Data Subject Access Request (or purported Data Subject Access Request);
 - 9.1.2 receives a request to rectify, block or erase any Personal Data;
 - 9.1.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - 9.1.4 receives any communication from any Supervisory Authority, including from the Information Commissioner's Office, or any other regulatory authority in connection with Personal Data processed under or in connection with this Agreement; or
 - 9.1.5 receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, and the Contractor will provide the Board with a copy of the relevant Data Subject Access Request, request, complaint or communication, as the case may be and such further information regarding the same as the Board may request from time to time.
- 9.2 Taking into account the nature of the Processing, the Contractor shall provide the Board with all reasonable assistance in relation to any complaint, communication or request notified to the Board pursuant to Clause 9.1 (and insofar as possible within the timescales reasonably required by the Board).
- 9.3 The Contractor shall, at its own cost and expense:

- 9.3.1 notify the Board of any Data Loss Event of which it becomes aware within twenty four (24) hours of becoming aware of such Data Loss Event; and
- 9.3.2 provide the Board, as soon as practicable and wherever possible within twenty four (24) hours of becoming aware of such Data Loss Event, with such information regarding the Data Loss Event as the Board may reasonably require, including but not limited to:
 - 9.3.2.1 the nature of the Data Loss Event, including, where possible the categories and approximate number of Data Subjects and Personal Data records affected by the Data Loss Event;
 - 9.3.2.2 the likely consequences of the Data Loss Event;
 - 9.3.2.3 where the Data Loss Event involves the Contractor and/or any Sub-processor, the measures taken or proposed to be taken by the Contractor and/or any Sub-processor to address the Data Loss Event, including those to mitigate the possible adverse effects of the Data Loss Event.

9.4 If the Contractor cannot provide all of the information set out in Clause 9.3 within the timescale specified, the Contractor shall, within such timescale advise the Board of the delay and of the reasons for the same and advise the Board when the Contractor expects to be able to provide the relevant outstanding information, which information may be provided in phases without undue delay, as details become available.

10 RECORDS

- 10.1 The Contractor shall maintain complete, accurate and up-to-date written records of all Processing carried out under or in connection with this Agreement. Such records shall contain the following information:
 - 10.1.1 the name and contact details of the Contractor's Representative (if any) and of the Contractor's Data Protection Officer (if any);
 - 10.1.2 the categories of Processing carried out on behalf of the Board;
 - 10.1.3 where applicable, details of any transfers of Personal Data pursuant to Clause 8.3, including the identity of the recipient of such transferred Personal Data and the countries to which such Personal Data is transferred, together with details of the Appropriate Safeguards used; and
 - 10.1.4 a general description of the Protective Measures implemented by the Contractor pursuant to Clause 6.1.

11 USE OF SUB-PROCESSORS

- 11.1 The Contractor shall not allow any Sub-processor to Process any Personal Data unless the Contractor has:
 - 11.1.1 notified the Board in writing of the intended Sub-processor and the Processing activity that the Contractor wishes the Sub-processor to undertake on the Contractor's behalf;
 - 11.1.2 obtained the prior written consent of the Board in respect of the use of such Sub-processor in connection with the Processing undertaken pursuant to this Agreement;
 - 11.1.3 entered into a binding written agreement with the Sub-processor, which agreement sets out enforceable data protection obligations on the same terms

as set out in this Agreement such that they apply to the Sub-processor, in particular such binding written agreement must provide:

11.1.3.1 sufficient guarantees that the Sub-processor will adopt Protective Measures such that the Processing undertaken by the Sub-processor will meet the requirements of the Data Protection Legislation; and

11.1.3.2 details of the Processing that is to be undertaken by the Sub-processor, which Processing shall only involve activity that is set out in the Schedule; and

11.1.4 provide the Board with such other information regarding the Sub-processor as the Board may reasonably require from time to time.

11.2 The Contractor shall cease using a Sub-processor to undertake any Processing of Personal Data pursuant to or in connection with this Agreement immediately upon receipt of a written request from the Board requesting that such Sub-processor ceases Processing the Personal Data, in circumstances where the Board has reasonable grounds for concern about the Sub-processor's ability to carry out the Processing in accordance with the Data Protection Legislation.

11.3 The Contractor shall remain fully liable for all acts or omissions of any Sub-processor.

12 AUDIT RIGHT

12.1 The Contractor shall, and shall procure that any and all Sub-processors shall, make available to the Board, at no cost or expense to the Board, all information necessary to demonstrate the Contractor's compliance with its obligations under this Agreement and the Data Protection Legislation.

12.2 The Contractor shall, and shall procure that any and all Sub-processors shall, allow for and contribute to audits, including inspections, conducted by the Board or by another auditor mandated by the Board, for the purpose of reviewing and assessing the Contractor's compliance with its obligations under this Agreement and the Data Protection Legislation, provided that the Board shall, where possible:

12.2.1 provide the Contractor with reasonable prior notice of such audit or inspection;

12.2.2 ensure that such audit is carried out during normal business hours; and

12.2.3 ensure that each such audit and inspection is carried out so as to cause minimal disruption to the Contractor's business and other customers.

12.3 The Parties agree that they shall bear their own respective costs and expenses incurred in respect of compliance with their obligations under Clause 12.2, unless the audit identifies a breach of the Contractor's obligations under this Agreement and/or the Data Protection Legislation, in which case the Contractor shall reimburse the Board for all of the Board's reasonable costs incurred in the course of the audit.

12.4 If an audit identifies that the Contractor has failed to perform its obligations under this Agreement in any material manner, the Board may, at its sole discretion:

12.4.1 treat such failure as a material breach of the Agreement; or

12.4.2 agree with the Contractor a remedial plan to resolve such failure, which remedial plan the Contractor shall implement at its sole cost and expense.

13 DELETION OR RETURN OF PERSONAL DATA

- 13.1 On termination of this Agreement, howsoever arising, or on the cessation of those Services pursuant to or in connection with which the Processing of Personal Data by the Contractor on behalf of the Board was undertaken, the Contractor shall immediately cease using all affected Personal Data in the possession or control of the Contractor
- 13.2 Within one (1) month following the date of termination of this Agreement, or if earlier, the date of the cessation of those Services pursuant to or in connection with which the Processing of Personal Data by the Contractor on behalf of the Board was undertaken, the Contractor shall, at the written direction of the Board, securely delete or securely return to the Board all affected Personal Data (and any copies of it) and the Contractor shall certify in writing to the Board that to the best of the Contractor's knowledge and belief all Personal Data (and any copies of it) have been securely deleted or securely returned to the Board, unless the Contractor is required by Law to retain the Personal Data. If the Contractor is required by Law to retain the Personal Data, the Contractor shall advise the Board of such requirement in writing.

14 LIABILITY

- 14.1 The Contractor shall indemnify and keep indemnified and defend at its own expense the Board from and against any and all DP Losses incurred by the Board or for which the Board may become liable arising from or in connection with any failure by the Contractor or any Sub-processor or any of their employees or agents to comply with any of the Contractor's obligations under this Agreement. The indemnity set out in this Clause 14.1 shall not be subject to any limit of liability
- 14.2 The Board shall indemnify and keep indemnified and defend at its own expense the Contractor from and against any and all DP Losses incurred by the Contractor or for which the Contractor may become liable arising solely from or in connection with any failure by the Board or its employees or agents to comply with any of the Board's obligations under this Agreement. The aggregate liability of the Board in respect of the indemnity set out in this Clause 14.2 shall in no event exceed an amount equivalent to TWO HUNDRED PERCENTUM (200%) of the fees paid by the Board for the Services in the 12 months prior to the event giving rise to the claim, notwithstanding any limit of liability in terms of Clause 14.

15 GENERAL

- 15.1 This Agreement shall terminate automatically upon the termination of the Services Agreement, Notwithstanding the provisions of this Clause 15.1, the provisions of Clauses 1, 3, 5, 9, 10, 13, 14 and 15 shall survive expiry or termination of this Agreement, howsoever caused.
- 15.2 Any notice to be given under this Agreement shall be delivered personally, sent by facsimile or sent by first class recorded delivery post (airmail if overseas) or electronic mail. The address for service shall be the registered or principal office of the recipient or such other address for receipt of notices as either Party may previously have notified to the other Party in writing. A notice shall be deemed to have been served:-
- 15.2.1 if personally delivered, at the time of delivery.
- 15.2.2 if sent by facsimile at the time of transmission.

15.2.3 if posted, at the expiration of forty eight (48) hours; and

15.2.4 if sent by electronic mail, at the time of the transmission.

- 15.3 In proving such service it shall be sufficient to prove that personal delivery was made, or that the envelope containing such notice was properly addressed and delivered into the custody of the relevant Party as prepaid first class or recorded delivery (as appropriate) or that the facsimile was transmitted on a tested line or that the correct transmission report was received from the facsimile machine sending the notice as the case may be, or that the hard drive has recorded the successful transmission of the electronic mail.
- 15.4 The Contractor shall not assign, sub-contract or otherwise transfer any of its Processing obligations in respect of the Personal Data to any third parties other than in accordance with the provisions of Clause 11.
- 15.5 The failure by either Party to insist upon the strict performance of any provision, term or condition of this Agreement or to exercise any right or remedy consequent upon the breach thereof shall not constitute a waiver of that Party's rights or remedies in respect of any such breach by the other Party or any subsequent breach of such provision, term or condition.
- 15.6 No waiver of any of the provisions of this Agreement shall be effective unless it is expressly stated to be a waiver and notified to the other Party in writing in accordance with the provisions of Clause 15.2.
- 15.7 This Agreement constitute the entire agreement between the Parties and supersede all previous discussions, correspondence, negotiations, arrangements, understandings and agreements between the Parties relating to the subject matter of this Agreement, provided that nothing contained herein shall operate or be construed as to limit or exclude either party's liability for fraud or fraudulent misrepresentation.
- 15.8 This Agreement shall be governed and construed in accordance with Scots law and both parties hereby irrevocably submit to the exclusive jurisdiction of the Scottish Courts: IN WITNESS WHEREOF, these presents consisting of this page and the preceding 12 pages are executed as follows:

For and on behalf of NHS Lothian

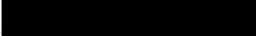
Place **Edinburgh**

Date **11 June 2024**

Signed by *Tracey Gillies*

Witnessed by 

Print Name **Tracey Gillies**

Print Name 

Designation **Executive Medical Director**

Designation **Business Support Officer**

Address **Waverley Gate, 2-4 Waterloo Place, Edinburgh EH1 3EG**

For and on behalf of Mellowood Medical Inc

Place **TORONTO CANADA**

Date **JUNE 3, 2024**

MellowoodMedical
ideas
 45 Mellowood Drive, Suite 18
 Toronto, ON
 Canada M2L 2E4

Signed by [Redacted]
Print Name [Redacted]

Witnessed by [Redacted]
Print Name [Redacted]

Designation PRESIDENT,
MELLOWOOD MEDICAL

Designation CONSULTANT
Address 45 MELLOWOOD DR.
TORONTO ON, CANADA
M2L 2E4

MellowoodMedical
idea
45 Mellowood Drive, Suite 18
Toronto, ON
Canada M2L 2E4

This is the Schedule referred to in the foregoing Data Processing Agreement between NHS Lothian and Mellowood Medical Inc

SCHEDULE

1. The Contractor shall comply with any further written instructions with respect to Processing issued by the Board.
2. Any such further instructions shall be incorporated into this Schedule.

| Description | Details |
|---------------------------------------|---|
| Subject matter of the processing | For Edinburgh Fertility Centre (EFC) to use IDEAS by Mellowood Medical Inc electronic patient record software for the management of patient fertility data. IDEAS will encourage 'paper-lite' working practice and reduce the clinical risks associated with using multiple sources of patient information. |
| Duration of the processing | Processing of personal data will be for the duration of the contract; this will be reviewed every 3 years. |
| Nature and purposes of the processing | <p>Staff will access the system via personal logins, each staff member will have restricted access depending on the level of access required for their job. These accounts will be managed in house by NHS Lothian.</p> <p>Personal data will be provided by the referring GP/clinician to allow the service to safely identify the patient/couple. The patient/couple will also be required to provide key information which will assist with their fertility investigations to ensure that they are contactable, and treatment is safe and appropriate.</p> <p>Patients' details will be manually entered onto IDEAS when the patient is added to the Artificial Reproductive Treatment (ART) waiting list. From then, any appointments, discussions, results and treatments will be updated on the patients IDEAS record manually by the appropriate clinic staff.</p> <p>Data will be collected from patients directly through a series of standardised forms and conversations with service staff.</p> <p>The Fertility Consents platform (currently used in NHS Lothian for sending consents and documentation to patients for sign off) will be integrated with IDEAS to ensure the signed</p> |

| | |
|--|--|
| | <p>documentation can be kept securely with the patient record.</p> <p>There will be a button within IDEAS that will trigger patient documents to be generated and some patient details will be transferred for their creation. Once signed documents are sent back by the patient, they can then be exported to be saved on the patient record within IDEAS.</p> |
| <p>Type of Personal Data</p> | <p>Patients – name, address, contact details, date of birth, age, Health data. Staff – name, work email address.</p> |
| <p>Categories of Data Subject</p> | <p>Patients Staff</p> |
| <p>Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data</p> | <p>For patients undergoing HFEA licensed treatment, the centre is legally required to retain their personal details and the details of their treatment for 30 years after last point of contact. This being 30 years after treatment or when no gametes or embryos are held in storage for them.</p> <p>For patients undergoing treatment which uses donor gametes or embryos, the service is legally required to store this data for at least 50 years.</p> |
| <p>Minimum Requirements</p> | <p>Remote access only permitted via HSCN/SWAN or Beyond Trust for remote access.</p> <p>Any changes to the transfer or storage of NHS Lothian PII data, to be approved by NHS Lothian IG/IT Security.</p> <p>All software (inc embedded) to be in current support and fully supported for the full lifecycle of the application.</p> |

Additional Information

Mellowood Medical Inc confirm that they are subject to the provisions of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and NHS Lothian accepts that as evidence of adequacy in respect of remote support operations conducted from the province of Ontario per The European Commission's adequacy decisions in relation to processing in Canada under PIPEDA in December 2001 (adopted by the UK following Brexit on 31 December 2020).

Mellowood Medical Inc may also provide remote support from its contracted staff in its other locations:

- Netherlands – remote support is provided from within the European Economic Area with no additional safeguards required.
- USA – remote support may be provided subject to the provisions of S.8.3 above. The Standard Contract Clauses provided in Schedule 2 below apply in respect of this processing activity.
- India – remote support may be provided subject to the provisions of S.8.3 above. The standard Contract Clauses provided in Schedule 2 below apply in respect of this processing activity.

Remote support may only be provided from sites directly controlled by Mellowood Medical Inc; by staff employed directly by Mellowood Medical Inc; and using equipment owned, operated, and secured by Mellowood Medical Inc.

No person employed by an agency or other sub-contractor is permitted to provide support without the prior express written permission of NHS Lothian responsible executive (currently the Medical Director, Caldicott Guardian or SIRO)

No sub-processors are permitted in respect of the processing envisaged by this agreement.

Data Processes and Flows

This document describes how Fertility Consent collects and processes patient data when used a Clinic Management System. Data is communicated via secure APIs, and Fertility Consent does not share any information outside the organisation.

Under UK Data Protection legislation and EU GDPR regulations MD Consents Limited, the providers of Fertility Consent, operates as a Data Processor on behalf of clients (who are the Data Controllers).

Our contract with clients (schedule 5: Processing, personal data and data subjects) describes our obligations under GDPR, what data is processed and how it is processed on the client's behalf.

Personal Data Collection and Storage

Fertility Consent collects 'demographic' information which is stored and used to populate the Clinic and HFEA forms.

It is also used to carry out important checks e.g. marital status, consent to storage periods, consent for research; where fields are inconsistent between patient and partner (if they have one) - alerts are raised for the clinic to investigate and respond to.

Once the consent case is archived the demographic information is deleted, and just the anonymised case / patient / partner / treatment data is retained for use in managing repeat cycles and for audit trail purposes.

Full privacy policy available online: <https://fertilityconsent.com/privacy>

Cookie policy available online: <https://fertilityconsent.com/cookies/>

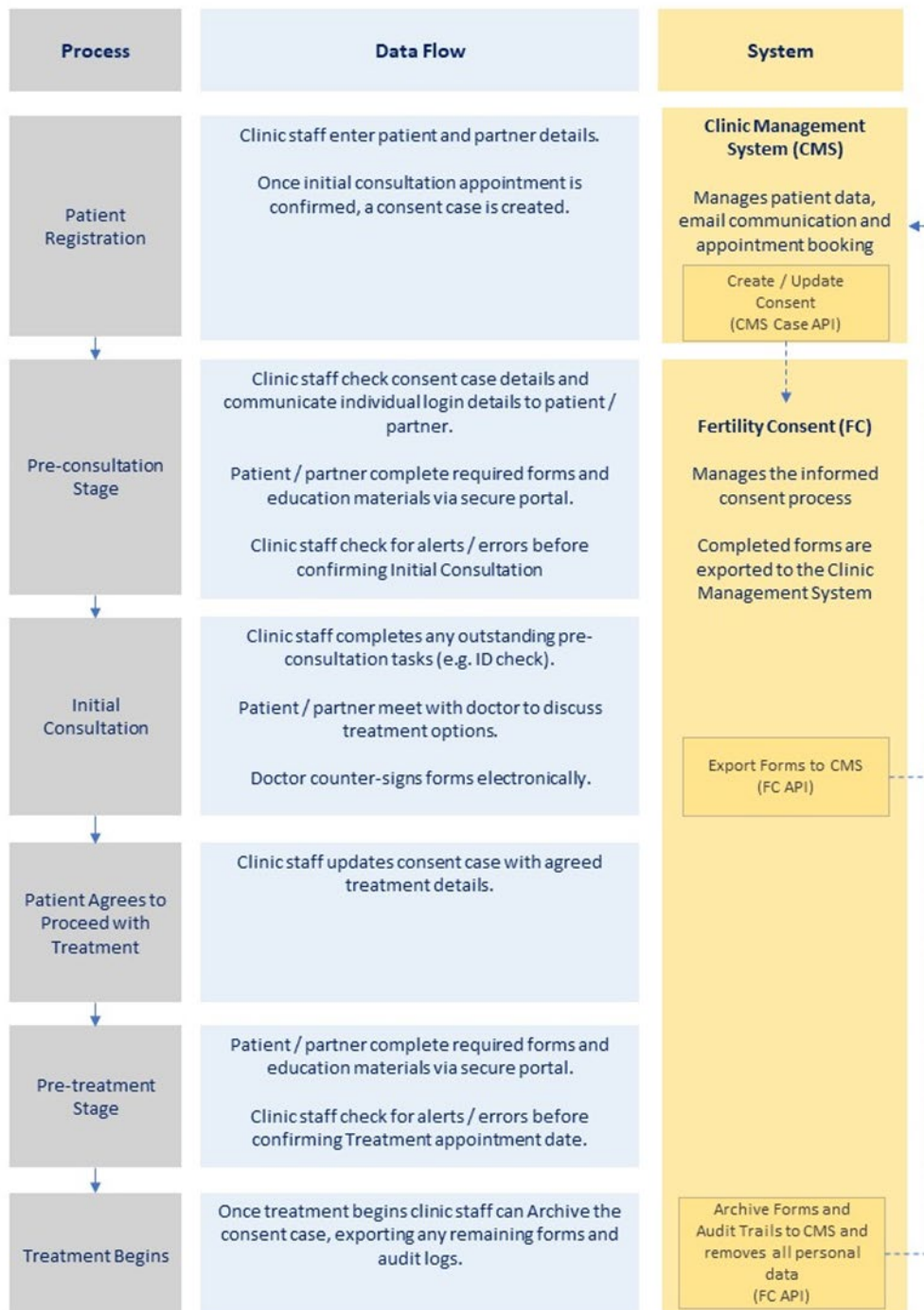
IG Information: Data Processes and Flows

Data Items stored and processed:

| | |
|-----------------------------------|---|
| Patient Data | Last update: August 8th 2023 |
| Purpose | Legal Basis |
| Patient Portal | Consent |
| | |
| Categories of personal data | Demographics, Identity Documents, Medical History |
| Categories of recipients | Contracted Customer |
| Retention | For duration of the consent process (Avg 3 mths, Max 12 mths) |
| Disposal | All Personal Data deleted after each treatment cycle |
| Other Sharing Agreements | None |
| Transfer Overseas | No |
| | |
| Main Patient Data Items | Optional Patient Data Items |
| Title | ID Document Type |
| First Name | ID Document Number |
| Middle Name | ID Document Image |
| Last Name | Country of Birth |
| Last Name at birth (if different) | Place of Birth |
| Date of Birth | Nationality |
| Occupation | |
| Sex | |
| Gender Identity | |
| Marital Status | |
| National Health Number | |
| Full Home Address | |
| Mobile Phone Number | |
| Email Address | |
| Medical History | |
| Ethnic Group | |
| Primary Language | |

Data Flows in conjunction with a Clinic Management System

The diagram below shows the main processes and system interfaces. Fertility Consent does not share any information outside the organisation.



Operational Processes

1. Data Storage:

Data is collected via online forms (browser) and stored (in encrypted format) in Microsoft Azure databases. All data transmitted between browsers and our servers, and our servers to Clinic systems are encrypted using a 256-bit encryption. Data at rest is also encrypted (see separated document for technical details).

2. Data Processing:

Data is manually entered and processed according to a set of algorithms which match the correct medical and legal forms and check for errors across patient / partner forms.

3. Data Quality:

All forms have validation to prevent basic user input errors. The algorithms mentioned above add an advanced level of checking specific business rules associated with fertility treatments.

4. Data Removal:

Once consent forms have been Exported and the consent case Archived – all data is then stored and managed in the clinic management system and subject to current data retention policies applicable there.

Fertility Consent retains the following high-level data associated with the consent case which is needed if there is a subsequent treatment cycle:

- Date Case Created / Case Number / Patient Number / Partner Number / Treatment Type
- Consent Notes and Audit Log
- Date Case Archived / Name of Person who Archived.

5. Data Backup:

Back-ups of all servers are taken daily, early morning between 01:00 and 06:00 GMT.

- Times vary by server due to the variance in time taken to copy each machine.

A standard Daily-Weekly-Monthly Backup is used:

- Daily: full backup set, one for each day of the week.
- Weekly: copy of 'day seven' backup archived to separate data centre at end of each week.
- Monthly: copy of 'final week' backup archived to separate data centre and optical media for off-site storage.

Back-ups are held for a period of 12 months; this allows for data recovery for any given day up to 1 month prior to the time of restore.

6. Data Redundancy:

All servers are backed up to the secondary data centre in Durham, and these back-ups can be used to recover the service in the event of a disaster on the core infrastructure.

Appendix – Archive Process

GDPR regulations dictate MDC only store personal data whilst we have a legitimate reason. For Fertility Consent we only hold detailed personal information whilst there is a current treatment is in progress.

Once the current treatment cycle is complete clinic staff must Archive the case which permanently removes all personal information, removes all completed forms and retains only high-level meta data - should the patient have a subsequent treatment cycle.

After Archiving a case, the high-level meta data retained is:

- Case Number
- Patient / Partner ID numbers
- Marital Status
- Fertility Treatment Type
- Source of Eggs / Sperm
- Case Summary of issued materials and forms
- Full Audit Trail of Clinic, Patient & Partner Activity
- Date Case Archived
- Clinic user who Archived case
- Archive Notes
- Archive Code

This high-level meta data (no personal data stored) is retained for 7 years, or the length of the contract between the Customer and MDC, whichever is the shorter.

Typically, there is a window of a few years when people undergo fertility treatments, this can be as short as 1 year, averages 3-4 years but has been known to extend to 5-6 years.

So, 7 years is the practical retention period to ensure the vast majority of re-occurring cycles are picked up correctly.

Appendix – Contract End – Data Destruction

Once a contract end date has been agreed, MDC will contact the customer 30 days before the agreed date to confirm the following process:

- Day 30:
 - Confirmation of intent to delete customer data and confirm who will sign-off from both the customer and MDC.
 - MDC to provide a summary of active cases on the platform. It is the customer's responsibility to Archive all cases before Day 0 (deletion day) to ensure that all completed forms, ID documents, and audit logs have been exported to their clinic management system or Azure storage area.
 - Agree a date to prevent patients from logging in to the clinic portal.
 - Outline the customer checks and actions before Day 0.

- Day 15:
 - MDC and customer review Archive process and re-confirm deletion date.

- Day 7:
 - MDC and customer review Archive process, identify any data not transferred to clinic management system or Azure storage area and re-confirm deletion date.

- Day 0:
 - MDC and customer agree to delete all related customer data. MDC will then delete all cases, forms, documents, users, clinic users, clinic details, and remove the customer account. MDC will confirm to the customer that these actions have been successfully completed and cannot be undone.

Deleting all data begins with removing all current and archived cases using a MDC admin feature. Once all case data is deleted, the clinic(s) and organisation are also removed by MDC Admin.



Data Protection Impact Assessment (DPIA) Questionnaire for

[IDEAS – Replacement EPR System for EFREC]

[Assessment date: March 2024]

[Review date: March 2026]

DOCUMENT CONTROL SHEET

Key Information

| | |
|-----------------------------------|--|
| Title | IDEAS – Replacement EPR System for EFREC |
| Date Published/ Issued | March 2024 |
| Date Effective From | March 2024 |
| Version/ Issue Number | 1 |
| Document Type | DPIA |
| Document Status | Approved |
| Author | ██████████ |
| Owner | ██████████ |
| Approvers | Information Governance |
| Contact | ████████████████████ |
| File Name | IDEAS – Replacement EPR System for EFREC |

Revision History

| Version | Date | Summary of Changes |
|---------|------------|---|
| V1 | 31/03/2023 | IG Update |
| V1.1 | 07/12/2023 | Update to DPIA by Service/Projects Team |
| | | |
| | | |
| | | |

Approvals

| Version | Date | Name | Designation |
|---------|------------|------------|--------------------|
| V1 | 14/03/2024 | ██████████ | IG Project Manager |
| | | | |
| | | | |
| | | | |
| | | | |

About the Data Protection Impact Assessment (DPIA)

The DPIA (also known as privacy impact assessment or PIA) is an assessment tool which is used to identify, assess and mitigate any actual or potential risks to privacy created by a proposed or existing process or project that involves the use of personal data. It helps us to identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. Failing to manage privacy risks appropriately can lead to enforcement action from the Information Commissioner's Office (ICO), which can include substantial fines. The DPIA is just one specific aspect of risk management, and therefore feeds into the overall risk management processes and controls in our organisation.

A DPIA is not a 'tick-box' exercise. Consultation may take a number of weeks to complete, so make sure that key stakeholders are engaged early, and that your project plan allows for this so that you have enough time prior to delivery to iron out any issues.

Carrying out a DPIA is an iterative process. Once complete, a review date within the next 3 years must be set. Should a specific change in purpose, substantial change in service or change in the law occur before the review date, the DPIA must be re-done.

The [ICO code of practice on conducting privacy impact assessments](#) is a useful source of advice.

Is a DPIA required?

If the process or project that you are planning has one or more the aspects listed below then you must complete a DPIA at an early stage.

| | | YES/NO |
|----|--|--------|
| 1. | <p>The work involves carrying out a systematic and extensive evaluation of people's personal details, using automated processing (including profiling). Decisions that have a significant effect on people will be made as a result of the processing.</p> <p><u>Includes:</u> Profiling and predicting, especially when using aspects about people's work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements Processing with effects on people such as exclusion or discrimination</p> <p><u>Excludes:</u> Processing with little or no effect on people</p> | No |
| 2. | <p>The work involves carrying out large scale processing of any of the special categories of personal data, or of personal data relating to criminal convictions and offences.</p> <p><u>Includes:</u></p> <ul style="list-style-type: none"> • Racial or ethnic origin data • Political opinions data • Religious or philosophical beliefs data • Trade Union membership data • Genetic data • Biometric data for the purpose of uniquely identifying a person • Health data • Sex life or sexual orientation data • Data which may generally be regarded as increasing risks to | Yes |

| | | YES/NO |
|----|---|--------|
| | <p>people's rights and freedoms e.g. location data, financial data</p> <ul style="list-style-type: none"> • Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive <p><u>To decide whether processing is large scale you must consider:</u></p> <ul style="list-style-type: none"> • The number of people affected by the processing, either as a specific number or as a proportion of the relevant population • The volume of data and/or the range of different data items being processed • The duration or permanence of the processing • The geographical extent of the processing activity | |
| 3. | The work involves carrying out large scale and systematic monitoring of a publicly accessible area . Includes processing used to observe, monitor or control people. | No |
| 4. | The work involves matching or combining datasets e.g. joining together data from two or more data processing activities performed for different purposes and/or by different organisations in a way that people would not generally expect; joining together data to create a very large, new dataset. | Yes |
| 5. | The work involves processing personal data about vulnerable groups . This includes whenever there is a power imbalance between the people whose data are to be used e.g. children, the mentally ill, the elderly, asylum seekers, and the organisation using their personal data. | Yes |
| 6. | The work involves significant innovation or use of a new technology . Examples could include combining use of finger print and face recognition for improved physical access control; new "Internet of Things" applications. | No |
| 7. | The work involves transferring personal data across borders outside the countries listed in the ICO website ? <ul style="list-style-type: none"> ✓ EEA countries ✓ Countries with an 'Adequacy decision' . You can view an up to date list of the countries which have an adequacy finding on the European Commission's data protection website. ✓ covered by the EU-US Privacy Shield framework. check on the Privacy Shield list to see whether the organisation has a current certification; or ✓ Covered by Canada's PIPEDA | No |
| 8. | The work involves processing that will prevent people from exercising a right or using a service or a contract e.g. processing in a public area that people passing by cannot avoid. | No |

Step One – Consultation Phase

Consult with all stakeholders about what you wish to do as early as possible in the process. Stakeholders will normally include:

- Key service staff e.g. those who will be managing the process.
- Technical support, especially if a new system is involved. This may involve the relevant IT supplier.
- Information governance advisors e.g. Caldicott Guardian, Information Security Officer, Data Protection Officer.

Sometimes it will be necessary to consult with service users. This will be particularly relevant if the change in process will change how they interact with our NHS Board, or what information is collected and shared about them.

Early consultation will ensure that appropriate governance and security controls are built into the process as it is being designed and delivered, rather than being 'bolted on' shortly before the change is launched.

Step Two- DPIA drafting

The responsibility for drafting a DPIA will normally sit with the service area that 'owns' the change, however, all stakeholders will have an input. Depending on the nature and complexity of your proposal, more than one service area and/ or Information Asset Owner (IAO) may be the owner(s).

Step Three- Sign-off

[NHS Board may need to also add in here specific, local/ administrative details on how DPIAs should be carried out and recorded in their organisation e.g. links with the Information Asset Register, mailboxes to use etc]

When a DPIA has been fully completed, it must be submitted for formal review by an appropriate IG professional/ the Data Protection Officer. They will review the DPIA to ensure that all information risks are fully recognised and advise whether appropriate controls are in place. The Data Protection Officer will decide, where the DPIA shows a high degree of residual risk associated with the proposal, whether it is necessary to notify the ICO. It may be necessary to inform and/or involve the Board's Senior Information Risk Owner (SIRO) as part of this risk assessment and decision-making.

Once reviewed, the DPIA will need to be signed off by the Information Asset Owner(s) (IAOs), normally a head of service.

1. **What are you trying to do and why? - give (or attach separately) a high level summary description of the process, including its nature, scope, context, purpose, assets e.g. hardware, software used, data-flows). Explain the necessity and proportionality of the processing in relation to the purpose(s) you are trying to achieve.**

Edinburgh Fertility Centre (EFC) requires a software solution that links two individuals as a couple and that cannot be accessed by staff outside the EFC due to the Human Fertilisation and Embryology Authority (HFEA) licence conditions. TRAK does not provide this functionality.

IDEAS by Mellowood Medical Inc is a specialised 'off-the-shelf' Electronic Patient Record software solution which meets the specific needs of the fertility service. The three other NHS fertility centres in Scotland are currently using IDEAS. Having a single unified platform across Scotland may support knowledge-sharing and provide dedicated performance analysis.

The implementation of IDEAS would replace EFC's current system, Filemaker, [REDACTED]

[REDACTED] The replacement of Filemaker would provide increased efficiencies and streamline processes within the department to enable EFC to provide better integrated care for patients.

IDEAS would encourage 'paper-lite' working practice and reduce the clinical risks associated with using multiple sources of patient information including Filemaker, paper medical records, paper diaries and excel spreadsheets.

IDEAS would also allow the service to:

- Schedule appointments
- Record patient communication
- Record medical history and progress notes.
- Store scans
- Record cycle details e.g., follicle count, endometrium size, medication, pathology results
- Management of frozen material e.g., sperm, eggs, and embryos
- Easily locate frozen material auditable
- Centralised embryo tracking
- Easily monitor performance and report on clinical indicators
- Track billing and payments
- Auditable electronic submissions to HFEA (PRISM) and error logs
- Provides traceability for consumables, equipment, and operators.

Staff will be able to access the system via personal logins and each staff member will have restricted access depending on the level of access required for their job. These accounts will be managed in house.

IDEAS will be integrated with Fertility Consents platform during the first phase to allow signed consent forms and other documentation to be attached to patient records on IDEAS. The fertility centre currently uses Fertility Consents platform for sending consents and documentation to patients for sign off. This will be integrated with IDEAS to ensure the signed documentation can be kept securely with the patient record.

Currently staff enter the details manually via the Fertility Consents web link and any subsequent documents are printed and saved with the patient's paper notes kept onsite. Integrating Fertility Consents with the new IDEAS solution will provide staff with a button within IDEAS that will automatically update patient details on Fertility Consents and any documents can then be exported and saved on the patient file on IDEAS.

Fertility Consents previously approved for use.

2. What personal data will be used?

| Categories of individuals | Categories of personal data | Any special categories of personal data [see Guidance Notes for definition] | Sources of personal data |
|----------------------------------|---|--|--|
| Patients | Name, Age, DoB, contact details, home address | Health data | Provided by Patient Provided by GP Trak Care |
| Staff | Name/email | None | Logging into the system |

3. What legal condition for using the personal data is being relied upon? [see Guidance Notes for the relevant legal conditions]

| Legal condition(s) for <i>personal data</i> [see Guidance Notes] | Legal conditions for any <i>special categories of personal data</i> [see Guidance Notes] |
|--|--|
| 6(1)(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 | 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional |

4. Describe how the personal data will be collected, used, transferred and if necessary kept up to date – may be attached separately.

Staff will access the system via personal logins, each staff member will have restricted access depending on the level of access required for their job. These accounts will be managed in house by two managers in the team (EFREC Unit Manager and Quality Manager) who have admin rights and are able to create and disable accounts where required.

Personal data will be provided by the referring GP/clinician to allow the service to safely identify the patient/couple. The patient/couple will also be required to provide key information which will assist with their fertility investigations to ensure that they are contactable, and treatment is safe and appropriate. **Partner details would still be collected/stored if a couple were to use a donor, however no identifiable information regarding the donor is stored within the system.** Patients are referred by GPs on TRAK initially and their details will be manually entered onto IDEAS when the patient is added to the Artificial Reproductive Treatment (ART) waiting list. From then, any appointments, discussions, results and treatments will be updated on the patients IDEAS record manually by the appropriate clinic staff.

Data will be collected from patients directly through a series of standardised forms and conversations with service staff. Patients are asked to confirm their contact details (including address) when they arrive for their appointments.

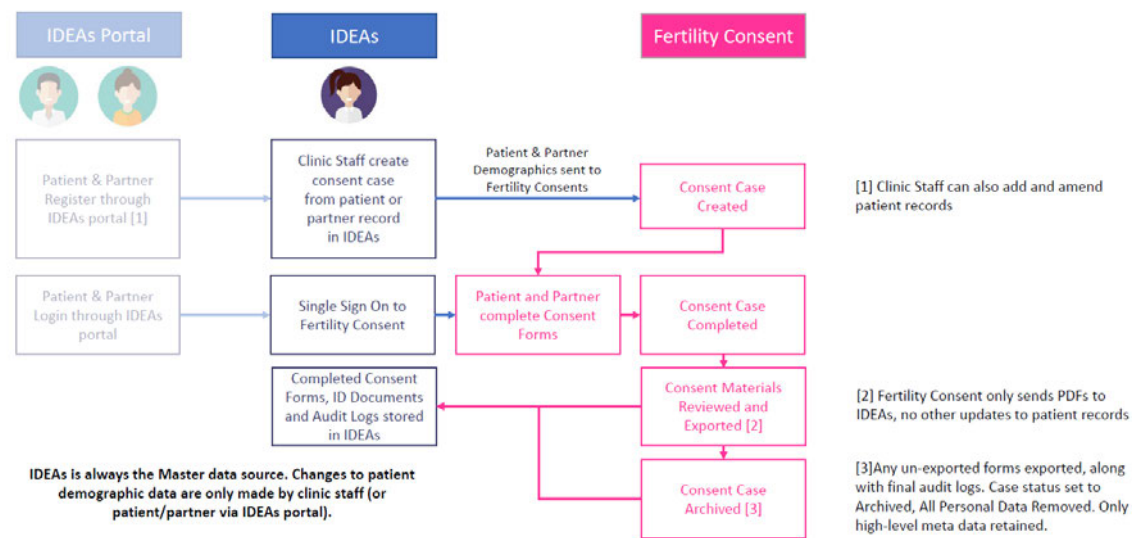
Prior to the sending of any patient correspondence, the service will continue to check stored information against Trak Care. **If a patient returns with a new partner, the previous relationship is unlinked, and the Service will link the new couple. Historic cycle data where previous partners were involved will remain in IDEAS with the partners reference – this data is not deleted, only suppress when providing the patient, a copy of their Patient Medical Record.**

Information will only be transferred to the HFEA via their reporting system PRISM. Staff manually enter this information on the PRISM web link. Admin staff have logins for this and enter patient and partner data such as Name, DOB, and some treatment data. This is a legal requirement. The Human Fertilisation and Embryology Act 1990 (as amended) requires all licensed centres to submit data to the HFEA. The proposed software is able to be linked directly to PRISM which will reduce unnecessary movement of patient information and transcription errors.

The fertility centre currently uses Fertility Consents platform for sending consents and documentation to patients for sign off. This platform will be integrated with IDEAS to ensure the signed documentation can be kept securely with the patient record. There will be a button within IDEAS that will trigger patient documents to be generated and some patient details will be transferred for their creation. Once signed documents are sent back by the patient, they can then be exported to be saved on the patient record within IDEAS.



IDEAs Integration – Basic Data Flow



5. **What information is being provided to the people to whom the data relate to ensure that they are aware of this use of their personal data? – This is the ‘right to be informed’ and information such as privacy notices may be included as an attachment.**

This new software will not require any additional information than what is already currently collected in paper form. Patients are given information around data protection, confidentiality and are given the address of the NHS Lothian Data Protection Notice.

[Data Protection Notice – Your Rights & Privacy \(nhslothian.scot\)](https://www.nhs.uk/lothian-trusts/lothian-data-protection-notice/)

Links to the Human Fertilisation and Embryology Authority for more information.

[HFEA: UK fertility regulator](https://www.hfea.gov.uk/)

[About us | HFEA](https://www.hfea.gov.uk/about-us/)

6. **How will people’s individual rights in relation to the use of their personal data be addressed by this process? (Rights are not applicable to all types of processing, and expert advice on this may be necessary.)**

- **Right of access:** Patients have the right to ask for a copy of any information NHS Lothian hold, requests will be dealt by the team within EFREC and reproduced following the SAR policy.
- **Right to rectification:** Data that is deemed incorrect can be rectified by NHS Lothian staff by updating the patient record.

- [Right to object](#) (where applicable): Patients have the right to object to processing in certain circumstances however this is not an absolute right. To exercise this right, individuals should contact the NHS Lothian Data Protection Officer who will consider each request on a case-by-case basis.
- [Right to restrict processing](#) (where applicable): Patients can object to processing which is necessary for the performance of NHSL tasks in the public interest or for the purpose of legitimate interests, NHSL will restrict the processing while it is considered whether our legitimate grounds override their individual interests, rights and freedoms.
- [Right to data portability](#) (where applicable): The right to data portability only applies when the individual has submitted their personal information directly, through electronic means to NHS Lothian. In this case it is not applicable.
- [Right to erasure](#) (where applicable): When using personal information, the legal basis is usually that its use is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us under the NHS Scotland Act as noted previously. This means that in most circumstances NHS Lothian will refuse requests for erasure.
- [Rights in relation to automated decision-making and profiling](#) (where applicable): Patients have the right not to be subjected to a decision, based solely on automated processing, including profiling. NHSL do not currently process any personal or company data in this way.

7. For how long will the personal data be kept?- refer to our Document Storage Retention and Disposal Policy for advice

For patients undergoing HFEA licensed treatment, the centre is legally required to retain their personal details and the details of their treatment for 30 years after last point of contact. This being 30 years after treatment or when no gametes or embryos are held in storage for them. For patients undergoing treatment which uses donor gametes or embryos, the service is legally required to store this data for at least 50 years.

Fertility Consent stores data until it is archived, once this happens the identifiable data is deleted, and anonymised data is retained for use in managing repeat cycles and audit purposes.

Fertility Consent only hold detailed personal information whilst there is a current treatment is in progress.

Once the current treatment cycle is complete clinic staff must Archive the case which permanently removes all personal information, removes all completed forms and retains only high-level meta data - should the patient have a subsequent treatment cycle.

This high-level meta data is retained for 7 years, or the length of the contract whichever is the shorter.

8. Who will have access to the personal data?

EFREC Staff and potentially some Mellowood staff who will be required to fill in the EFREC centre confidentiality agreement beforehand and all work will be done using Beyond Trust remote access session.

9. Will the personal data be routinely shared with any other service or organisation? – if yes, provide details of data sharing agreement(s) and any other relevant controls. Advice on data sharing requirements is in the [Scottish Information Sharing Toolkit](#).

Information will only be transferred to the HFEA (government body) via their secure reporting system PRISM. This is a legal requirement, and the proposed software is able to be linked directly to PRISM which will reduce unnecessary movement of patient information and transcription errors.

10. Will the personal data be processed internally by an internal Data Processor or externally by an external Data Processor e.g. an IT services provider? – [see [Guidance Notes for the definition of Data Processor](#)]. Provide details of contractor selection criteria, processing instructions and contract (may be attached separately).

Data will be processed internally with the system being supported remotely by Mellowood Medical. Mellowood would have limited access to personal data when remote accessing data for support purposes.

11. Describe what organisational controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary.)

| | |
|------------|------------|
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |

| Type of Control – examples | Description |
|----------------------------|-------------|
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |

12. Describe what *technical* controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary).

| Type of Control – examples | Description |
|----------------------------|-------------|
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |

| Type of Control – examples | Description |
|----------------------------|-------------|
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |

13. Will personal data be transferred to outside the [European Economic Area \(EEA\)](#) or countries [without an European Commission-designated adequate level of protection](#)? – if yes, provide details of the safeguards that will be in place for the transfer(s).

No data will be transferred outside the UK

14. Describe who has been consulted in relation to this process – e.g. subject matter experts, service providers, service users.

Quality Manager

EFREC management

15. In light of what is proposed, indicate what level of risk has been identified in relation to the following data protection principles:

| <i>Principle</i> | <i>Low/ Green</i> | <i>Medium/ Amber</i> | <i>High/ Red</i> |
|--|-----------------------|--------------------------|----------------------|
| Personal data is processed in a fair, lawful and transparent | x | | |

| <i>Principle</i> | <i>Low/ Green</i> | <i>Medium/ Amber</i> | <i>High/ Red</i> |
|---|------------------------------|---------------------------------|-----------------------------|
| manner | | | |
| Personal data is collected for specific, explicit and legitimate purposes | x | | |
| Personal data is adequate, relevant and limited to what is necessary | x | | |
| Personal data is accurate, and kept up to date | x | | |
| Personal data is kept no longer than necessary | x | | |
| Personal data is processed in a manner that ensures adequate security | x | | |

16. Risks and actions identified [see Guidance Notes for more information]. List all that you have identified and ensure that these integrate properly with our NHS Board’s risk management process:

| Description | Likelihood | Consequence | Overall Risk rating (LxC) | Mitigation/ Actions | Residual Risk | Risk Owner | Date |
|-------------|------------|-------------|---------------------------|---------------------|---------------|------------|------------|
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |

17. Review and Sign-Off

| Role | Advice/ Action/ Sign-Off | Date |
|--|---------------------------------|--|
| IG/ Data Protection (DPO) Advice | [REDACTED] | 31/03/2023 19/12/2023 14/03/2024 |
| | [REDACTED] | 14/03/2024 |
| Information Security Officer Advice (questions 11 and 12) | [REDACTED] – IT Security SSP | 27/02/2024 |
| Others, if necessary e.g. Caldicott Guardian, Senior Information Risk Owner (SIRO) | | |
| DPO opinion on whether residual risks need prior notification to the ICO | No ICO notification required | |
| Project Lead | [REDACTED] – Project Officer | 19/12/2023 |
| Information Asset Owner(s) (IAO(s)) Sign Off | [REDACTED] | 14/03/2024 |

18. Recommended Review Date: March 2026

GUIDANCE NOTES

Question 2 - Special category personal data

The special categories of personal data are specified in Article 9 of the General Data Protection Regulation and include data about:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a person
- health
- sex life or sexual orientation.

Personal data relating to criminal convictions and offences should be regarded as having the same special nature as those in the categories listed above.

Question 3 – Legal condition

It is illegal to process personal data without meeting adequately a legal condition.

For personal data which does not relate to any of the special categories (see definition above) the legal basis for the proposed processing must be one or more from the following list. Please note that 'data subject' means the person to whom the personal data relates.

- 6(1)(a) – Consent of the data subject
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- 6(1)(c) – Processing is necessary for compliance with a legal obligation
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
- 6(1)(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
- 6(1)(f) – Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

In NHS Scotland, in many cases condition 6(1)(e) will be the most relevant.

For personal data which relate to any of the special categories (see definition above) the legal basis for the proposed processing must be one or more from the following list:

- 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

- 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- 9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
- 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- 9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

In NHS Scotland, in many cases condition 9(2)(h) will be the most relevant.

The Information Commissioner's Office (ICO) advises that public authorities will find using consent as a legal basis difficult. So if the proposed processing is to use consent as its legal basis you need to indicate why this is necessary and seek the advice of an appropriate IG professional.

Question 10 – Data Processor

Article 4 of the General Data Protection Regulation defines a Data Processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller. In practice it includes organisations and companies that provide services such as records storage, transport and destruction and IT services, where we ask them to carry out specific tasks using personal data on our behalf. IT suppliers, even if only accessing data/systems for support issues or bug fixes, are legally defined as a Data Processor. Data Processors may only be used to process personal information where they have provided sufficient guarantees to implement appropriate technical and organisational measures to comply with the law.

Question 16 – Risk Assessment

ASSESSING THE LEVEL (GRADE) OF THE RISK

1. Determine the **Likelihood (L)** of recurrence for the event using **Figure 1** (see below).

When determining the likelihood you should consider:

- The frequency of any previous occurrences e.g. How many times a data breach was reported due to this type of issue (e.g. lost records or records accessed without authorisation) in the last month ? in the last year? In the last 5 years?
- You may need to check the Information Governance, Data Protection and Information Security incidents reported in your organisation in order to assess the likelihood.

Figure 1: Likelihood of Recurrence definitions

| Descriptor | Remote | Unlikely | Possible | Likely | Almost Certain |
|-------------------|---|--|---|---|--|
| Likelihood | Can't believe this event would happen – will only happen in exceptional circumstances (5-10 years) | Not expected to happen, but definite potential exists – unlikely to occur (2-5 years) | May occur occasionally, has happened before on occasions – reasonable chance of occurring (annually) | Strong possibility that this could occur – likely to occur (quarterly) | This is expected to occur frequently / in most circumstances – more likely to occur than not (daily / weekly / monthly) |

2. Determine the **Consequence (C)** rating using **Figure 2** (see below)

Look at **events** that could lead to the consequence, **not the consequence itself**

e.g. Examples of **Events**:

- Records lost in transit (e.g. paper records sent by post)
- Information recorded inaccurately or not recorded in the record
- Data not available due to ransom-ware attack
- Data lost due to error in IT systems – no useful backup available.
- Confidential personal data sent by email to wrong addressee
- Confidential personal data made available to external people due to poor role access definition and testing
- New system or changes in a system went live without appropriate change management (new or changes in data processing started without IG approval)

Examples of Consequences

- Only 1 data subject affected but significant or extreme consequences e.g. missed vital treatment as a consequence of information not being issued to the patient or health professional leading to death or major permanent incapacity
- very sensitive data being exposed to people who don't need to know causes extreme distress (could be patient or staff data)
- Large amount of non-sensitive but personal identifiable data lost in the wind when in transit causing organisational embarrassment in the news for a week
- Staff snooping on neighbours medical records
- Excessive health data shared with social worker (husband under domestic abuse investigation) causing direct threats and stalking.
- Personal health data shared by a charity with private business for commercial/marketing purposes causing unwanted disturbance.
- Reportable data breach to ICO causing monetary penalty.
- Complaint from patient to ICO results in undertaking for better access to health records.
- 1.6 million patients in Google Deepmind affected by the processing
- Compliance Audit recommended
- DC action required
- Undertaking served
- Advisory Visit recommended
- Improvement Action Plan agreed
- Enforcement Notice pursued
- Criminal Investigation pursued
- Civil Monetary Penalty pursued

When considering the consequences of a data breach in your proposed service/system which consequence should you opt for?

Don't choose the worst case scenario or the most likely scenario, but opt for the "**Reasonably foreseeable, worst case scenario**" where if you got a phone call to tell you it had happened, you wouldn't be surprised.

Figure 2: Consequence Table

| Descriptor | Negligible | Minor | Moderate | Major | Extreme |
|--|---|--|---|--|--|
| Objectives / Project | Barely noticeable reduction in scope / quality / schedule of an eHealth innovation (e.g. new system) | Minor reduction in scope / quality / schedule | Reduction in scope or quality, project objectives or schedule | Significant project over-run | Inability to meet project objectives, reputation of the organisation seriously damaged (e.g. Care Data) |
| Injury (Physical and psychological) to patient / visitor / staff. e.g. issues with data quality, availability or confidentiality with physical or psychological consequence for the data subject. | Adverse event leading to minor injury not requiring first aid (e.g. data quality issues on instruction to patient re prescription) | Minor injury or illness, first aid treatment required | Agency reportable, e.g. Police (violent and aggressive acts) Significant injury requiring medical treatment and/or counselling. e.g. Staff member who attempted suicide, privacy compromised as A&E shared details beyond "need-to-know". | Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling. | Incident leading to death or major permanent incapacity (e.g. health records not released on time for making treatment decision causing death or major injury). |
| Patient Experience e.g. poor access to my records or difficulties to exert data protection rights. | Reduced quality of patient experience / clinical outcome not directly related to delivery of clinical care | Unsatisfactory patient experience / clinical outcome directly related to care provision – readily resolvable | Unsatisfactory patient experience / clinical outcome, short term effects – expect recovery <1wk | Unsatisfactory patient experience / clinical outcome, long term effects – expect recovery - >1wk | Unsatisfactory patient experience / clinical outcome, continued ongoing long term effects |
| Complaints / Claims e.g. Complaints due to data protection issues | Locally resolved verbal complaint | Justified written complaint peripheral to clinical care | Below excess claim. Justified complaint involving lack of appropriate care | Claim above excess level. Multiple justified complaints | Multiple claims or single major claim |
| Service / Business Interruption e.g. from constant small interruptions of ICT systems to big Business Continuity issues due to cyberattacks or core data centre being down beyond acceptable levels. | Interruption in a service which does not impact on the delivery of patient care or the ability to continue to provide service | Short term disruption to service with minor impact on patient care | Some disruption in service with unacceptable impact on patient care Temporary loss of ability to provide service | Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked. | Permanent loss of core service or facility Disruption to facility leading to significant "knock on" effect |

| | | | | | |
|--|---|--|--|---|---|
| Staffing and Competence e.g. Poor data protection, confidentiality and ICT security training | Short term low staffing level temporarily reduces service quality (less than 1 day) Short term low staffing level (>1 day), where there is no disruption to patient care | Ongoing low staffing level reduces service quality Minor error due to ineffective training / implementation of training | Late delivery of key objective / service due to lack of staff. Moderate error due to ineffective training / implementation of training Ongoing problems with staffing levels | Uncertain delivery of key objective / service due to lack of staff. Major error due to ineffective training / implementation of training | Non-delivery of key objective / service due to lack of staff. Loss of key staff. Critical error due to ineffective training / implementation of training |
| Financial (including damage / loss / fraud) e.g. derived from compensation rights as per DPA, ICO or NIS fines, ransomware, etc. | Negligible organisational / personal financial loss (£<10k) | Minor organisational / personal financial loss (£10k-100k) | Significant organisational / personal financial loss (£100k-250k) | Major organisational / personal financial loss (£250 k-1m) | Severe organisational / personal financial loss (£>1m) |
| Inspection / Audit e.g. ICO or NIS interventions | Small number of recommendations which focus on minor quality improvement issues | Recommendations made which can be addressed by low level of management action. | Challenging recommendations that can be addressed with appropriate action plan. | Enforcement action. Low rating Critical report. | Prosecution. Zero rating Severely critical report. |
| Adverse Publicity / Reputation e.g. media attentions due to data breaches or cybersecurity attacks | Rumours, no media coverage Little effect on staff morale | Local media coverage – short term. Some public embarrassment. Minor effect on staff morale / public attitudes. | Local media – long-term adverse publicity. Significant effect on staff morale and public perception of the organisation | National media / adverse publicity, less than 3 days. Public confidence in the organisation undermined Use of services affected | National / International media / adverse publicity, more than 3 days. MSP / MP concern (Questions in Parliament). Court Enforcement Public Enquiry |
| Privacy | Negligible harm to the individual arising from disclosure of confidential or sensitive information. | Minor harm to the individual arising from disclosure of confidential or sensitive information. Uncomfortable situation with no material detrimental effect on the person. Minor impact on dignity. | Moderate harm to the individual arising from disclosure of confidential or sensitive information e.g. damage to personal relationships and social standing arising from disclosure of confidential or sensitive information | Major harm to the individual arising from disclosure of confidential or sensitive information e.g. ID theft with potential adverse effect to the individual for which the person is likely to recover overtime or significant loss of personal | Extreme harm to the individual arising from disclosure of confidential or sensitive information e.g. ID theft with financial loss extreme adverse effect or losing a job or Extreme risk to life or health |

V201901

| | | | | | |
|--|--|--|--|---|--|
| | | | | autonomy detrimental impact on dignity | |
|--|--|--|--|---|--|

Based on: Australian/New Zealand Standard: Risk Management (AS/NZS4360:2004 Risk Management Standard), (2004) Standards Australia/Standards New Zealand

Clinical Governance and Risk Management Standards (2005), NHS Quality Improvement Scotland

3. Use the risk matrix shown in **Figure 3** below to determine the risk grading for the risk. **L x C =R**

Figure 3: Risk Assessment Matrix

| <u>Likelihood</u> | Consequence | | | | |
|-----------------------|-------------|-------|----------|-------|---------|
| | Negligible | Minor | Moderate | Major | Extreme |
| Almost certain | LR | MR | HR | HR | HR |
| Likely | LR | MR | MR | HR | HR |
| Possible | VLR | LR | MR | MR | HR |
| Unlikely | VLR | LR | LR | MR | MR |
| Remote | VLR | VLR | VLR | LR | LR |

In terms of grading risks, the following grades have been assigned within the matrix.

- Very Low Risk (VLR)
- Low Risk (LR)
- Moderate Risk (MR)
- High Risk (HR)