# DATA PROTECTION IMPACT ASSESSMENT TEMPLATE (DPIA)[1]

**Research Technology Platform**

uMed provides technology enabled services to GPs that enable them to participate in more research programmes without creating additional burden to practice staff. uMed achieves this by acting on behalf of the practice under a data processing agreement to undertake a number of functions.

**Overview of services delivered by uMed**

1. **Potential participant identification, screening and trial site referral**
   This includes:

   Part A: Once the data processing agreement is in place
   a. Extraction and hosting of practice data using the NHS Digital IM1 pairing process
   b. Processing of data to separate pseudonymised health record data from patient contact information
   c. Applying queries to this data to identify potential participants within the practice and presenting this information back to the practice via uMed's portal

   Part B: *Only* when the practice agrees to participate in a specific study
   a. Engagement of patients by SMS, letter and email channels to inform them of study opportunity
   b. Collection of additional data via digital questionnaires and manual screening with uMed nurses to assess eligibility
   c. Obtain consent from patients for the practice to share contact information with the clinical trial site so that they can be contacted for enrollment
   d. Transfer of this contact information to the trial site using using the uMed platform

   **The above activity is covered by this DPIA.**
   **The legal basis for this processing is PUBLIC TASK**

2. **Additional study specific activity**

   uMed may also undertake study specific activity on behalf of the GP practice, where protocol defined activity is delegated to uMed. The additional written instruction to uMed which describes the processing activity will be provided to the practice as a statement of work (SOW) which will require review and agreement by the practice.

   Examples of study specific activity include:

   a. Capture of remote consent for participation in research
   b. Capture of patient reported outcomes as defined by the study protocol (e.g. symptom diaries)
   c. Sharing of data from the participant health record and/or sharing of additional data captured as part of the study with the study sponsor, as defined in the ethically approved protocol

Note: **Activity that is not covered by this DPIA,** supplementary information added on question 4e) and will be provided to the practice alongside the study specific statement of work which will describe the processing for a given study. **The legal basis for sharing any data with a third party study sponsor is CONSENT.**

[1] *"Where a type of processing using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller/processor shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."*

**The DPIA Process**

The Data Protection Act is mainly concerned with the disclosure of personal data outside the data controller's and/or processor's own boundaries.[2]

*If the data is to be **anonymised** **PRIOR** to any processing, we may not need to complete this DPIA and should review:*

- *question 1.20*
- *section 2*

and liaise with the Compliance Department to confirm completion is not required.

**Otherwise**:

1) Please complete each section by liaising with relevant stakeholders.
2) Once DPIA is submitted to the Compliance Department and all the sections are approved, then the DPIA will be signed off by the DPO.
3) Once approved, the process / system can start to be introduced or modification to an existing system / process can continue.

| | |
|---|---|
| **Initiative/System/ Process name:** | uMed Technology Platform |
| **Date Initiative due to go live/commenced:** | [Insert Date] |
| **Date DPIA commenced / Reviewed:** | 29/09/2022 |

[2] ICO – Anonymisation code

| DPIA Contact Details: *Please list all main contacts involved in completing the DPIA* | | | |
|---|---|---|---|
| **Name** | **Role** | **Department** | **Email** |
| **Matt Wilson** | **DPO** | **Management** | **matt@umed.io** |
| **Abi Dhillon** | **VP Commercial Operations** | **Operations** | **abi@umed.io** |
| **Sian Organ** | **Senior Project Manager** | **Operations** | **sian@umed.io** |
| **Chris Broderick** | **CTO** | **IT** | **chris@umed.io** |
| **Teresa Latta** | **Head Quality & Compliance** | **Compliance** | **teresa@umed.io** |

## Section 1: Project Information

**Description, purpose of and reason for the initiative (GDPR Art. 35(7)):** *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

**1.1 Description, purpose and benefits:**
uMed platform acts on behalf of the patient's healthcare provider to automate the process of conveying study communications to patients, as well as data to 3rd parties as part of HRA approved research studies. Authority will be sought from the data controller and – if necessary - consent from the data subject on a per study basis for this activity. This enables healthcare providers to participate in more research programmes without increasing burden.

**1.2 How will we collect the data?**
By integration with the GP practice(s) record system(s) and through digital questionnaires sent to the patients via electronic format.

**1.3 How will we use the data?**
Data will be used to provide services to the practice as described in the data processing agreement uMed has in place with the practice. These services include the use of this data to match patients to relevant research opportunities and present these back to the practice for consideration. If a practice chooses to join a research project, the study protocol and associated uMed schedule of work will define what further study specific use of data is required.

**1.4 Where and for how long will the data be stored?**
Data will be retained as stated on the uMed Platform Data Processing Agreement signed between the GP practice and uMed.

**1.5 What processes will be in place to delete the data when it is no longer required to be retained?**
Patient data belonging to a practice or study can be easily removed by an administrator inline with the requirements of the study. All data is stored electronically and available via the admin panel of the "Stern" study management platform (this includes identifiable data such as contact information, other collected data like responses to surveys, and contact history). Given enough information to uniquely identify an individual patient or group of patients, all data can be displayed online and reviewed/confirmed for deletion.

**1.6 What is the source of the data? E.g. the individual themselves, 3rd party**.
Practice electronic health record systems, NHS Digital, individuals.

**1.7 Will we be sharing the data with anyone? If yes, specify which organisation/team and the purpose of the sharing**
Data will be shared with uMed under the terms and purpose described in the data processing agreement. No 3rd party will be granted access to data unless a supplement to this DPIA is in place that will be provided on a study by study basis in accordance with the ethically approved protocol. A separate study agreement between the practice and the study sponsor will be required which will include details of any data sharing and associated terms.

**Description, purpose of and reason for the initiative (GDPR Art. 35(7)):** *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

**1.8 Specify the demographic/cohort/criteria.**
All patients registered to the practice

**1.9 Specify the area(s) within the UK or UK wide:**
UK wide.

**1.10 Specify any other organisations involved in the processing (*include any suppliers of e.g. databases*):**
Amazon Web Service (Secure cloud infrastructure); Twilio UK Limited or Firetext (text messaging); EMIS Group (data extraction service), TPP (data extraction service), Docmail (Letter sending service)

**1.11 What contractual arrangements are in place (specify contract terms or embed or attach relevant sections of contract/SLA?**
GEN12-uMed Platform User Terms and Conditions[3]
GEN13-uMed Platform Data processing Agreement[3]

**1.12 How often will you be collecting and using the personal data?** Ongoing until the end of contract.

**1.13 How long do you expect this initiative to last?**

☑ End of contract period

☐ Specific time period – specify?

☐ Lifetime of system (where the initiative or project relates to a new or revised ICT system)

☐ Other – specify …….. Click here to enter text

**1.14 What is the nature of your relationship with the individual data subjects for this initiative? (*This enables uMed to ascertain the lawful basis for processing)***

Provision of health/social care ☑ Protecting the health of the general public ☐

Local audit to assure safe health and social care ☐ Checking quality of care, beyond local audit ☐

Supporting research ☑ Staff employment ☐ Other - specify:.

**1.15 How much control will the data subjects have over the data being processed?**
Data subjects can opt out of processing by uMed by informing their GP who will add the relevant opt out codes to their records. Patients can also register for the national data opt out. All engagements provided to patients will include details of the opt out.

Once they have opted-out. No further processing of that individual's data will take place and data will be deleted from the uMed hosted database (see flow diagram in section 3). Additionally, For each study, data subjects will be informed of the planned processing and will be required to explicitly consent to this.

**1.16 Would they expect you to use their data in this way?**
Yes ☑ No ☐ Don't know ☐
The HRA provides clear guidance that processing for research is a public task and is part of the NHS constitution. Furthermore, data subjects are proactively engaged for consent to any study specific processing or third party data sharing.

**1.17 How will you consult with them to seek their views on the data processing – or justify why it is not appropriate to do so:** Guidance on consent and data privacy notice provided to GPs to place on their website and also present on uMed website. Data subjects are proactively engaged for consent to any study specific processing or third party data sharing.

**1.18 Do you need to consult with anyone else internally or externally?**

[3] Documents available upon request

**Description, purpose of and reason for the initiative (GDPR Art. 35(7)):** *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

Internally - Practices will review and approve each study opportunity presented through the uMed platform and externally the UK research and ethics committee will review all studies including aspects of patient data use and privacy.

**1.19 Will an individual's personal information be disclosed outside of the parties to this initiative in identifiable form and if so to who, how and why?**

☑ **Yes – provide details below** **No** ☐

uMed may also undertake study specific activity on behalf of the GP practice, where this activity has been delegated to uMed and additional written instruction provided to uMed which describes the additional processing activity that will be required. This will be provided to the practice as a statement of work (SOW) which will require review and agreement by the practice. In this case an amendment to this DPIA will be added for the specific study.

**1.20 If the information is to be anonymised or pseudonymised in any way, specify how this will happen**

Data is only shared with 3rd parties in pseudonymised form unless exclusions[2] apply. EHR records are stored within the uMed system as pseudonymised data. Software processes using an encryption firewall to separate the patient identifiable information from the health records at the time of ingestion and de-anonymising requires access to a number of encryption keys and software algorithms.

**1.21 If personal data is being transferred outside of the EEA, describe how the data will be adequately protected (e.g. the recipient is in a country which is listed on the Information Commissioner's list of "approved" countries - see link here, or how the data is adequately protected).** *(This would include database/information hosted on ICT applications outside the UK)*

Not applicable – data not being processed outside the UK ☑

**1.22 Are there any approved national codes of conduct or sector specific guidelines that apply to the data e.g. ICO/DoH&SC/NHS England/NHS Digital etc. (GDPR Art. 35(8))**

NHS Digital (ODS 8K677)
Codes of practice for handling information in health and care
IM1 Pairing Process
ICO-Anonymisation managing data protection risk code of practice
National Data Opt - Out

**1.23 How will you prevent function creep i.e. the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy?**

Strict controls in line with ISO27001:2013 certification criteria (Information Security)
All studies supported will require UK research and ethics approval and include a detailed study protocol describing if / how data is used. This DPIA will remain under uMed monitoring and review processes to ensure that any future development or wider out is appropriately governed. Specific studies will have their own DPIA appendix in place to ensure due process is undertaken to monitor and review in accordance with SOW.

**1.24 How will you ensure data quality?**

uMed is certified with ISO9001:2015 Quality Management Systems and ISO27001:2013 Information Security Management Systems, to ensure data quality through good data governance and rigorous data management.
uMed Technology Platform is designed to examine data to a rigorous data profiling on incoming data; avoids duplicate data; enables accurate gathering of data requirements for different studies; database rationale to enforce data integrity; integration of data lineage traceability into data pipelines; quality assurance and production quality control.

Section 2: Data Items

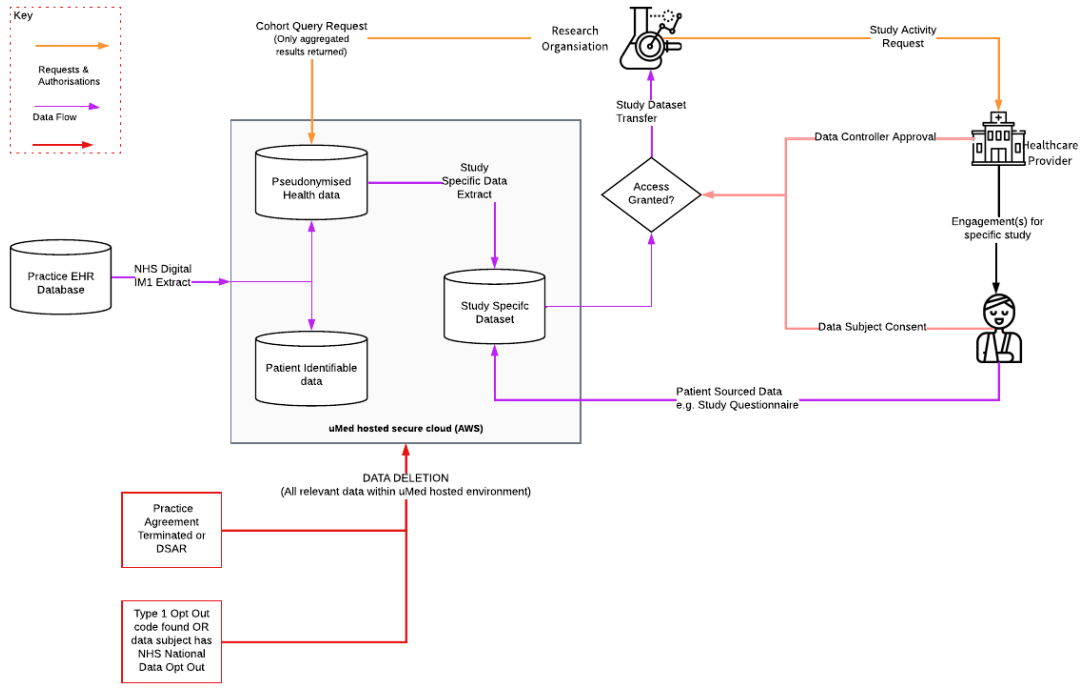
| Specific data item(s) |
|---|
| **Personal details -** Check all that apply:<br><br>☑ Forename(s) ☑Surname ☑Address ☑Postcode (full) ☐ Postcode (partial) ☑Date of Birth ☑ Age ☑ Gender<br><br>☐ Physical description ☑ Home Telephone Number ☑ Mobile Telephone Number ☐ Other Contact Number<br><br>☑ Email address ☑GP details ☐ Legal Representative Name (Next of Kin) ☑NHS Number ☐ National Insurance No.<br><br>☐ Photographs/Pictures of persons ☐ Location data e.g. IP address<br><br>☐ None of the above ☐ Other – List any other data items or attach as an appendix<br><br>Additional Items:<br>Electronic Health record data held by the GP<br>Health related information captured through digital engagement with the data subject |
| **Justification and compliance with data minimisation principle**<br>Reason that the data items(s) above are needed including any consultation/checks regarding the data items being adequate, relevant and limited to what is necessary – this must stand up to scrutiny |
| This information is required in order for uMed to provide its services either to GP's questioning and/or for searching across relevant data for patient matching for specific studies. |

| Other data item(s) | Justification and compliance with data minimisation principle<br>Reason that the data items(s) are needed including any consultation/checks regarding the data items being adequate, relevant and limited to what is necessary – this must stand up to scrutiny |
|---|---|
| Information relating to the individual's **physical or mental health or condition**.<br>*NB. For mental health this would include the mental health status i.e. whether detained or voluntary under the Mental Health Act.*<br><br>☑ Yes<br>☐ No<br><br>List any data items or embed document or attach as an appendix<br><br>Data elements received by uMed are determined by the exact schema defined with the electronic health record vendors (e.g EMIS), through the IM1 Pairing Process. | This information is required in order for uMed to provide its services either to GP's questioning and/or for searching across relevant data for patient matching for specific studies. |
| Information relating to the **family of the individual and the individual's lifestyle and social circumstances**<br><br>☑ Marital/partnership status<br>☑ Carers/relatives<br>☑ Children/dependents<br>☐ Social status e.g. housing<br>☐ Other – please specify below:<br>☐ None of the above | This information is contained within the extract provided to uMed under the NHS Digital IM1 Pairing process, and is required to identify NOK / dependents for engagement for specific studies |

**Section 3 – Data Flows** – *Identify each flow of data involved and document specific security measures in place.*

| Flow Ref | Flow name/description | Going from | Going to | Method of access /transfer and control | Specify the security control(s) in place for the flow | Where will the data be stored after access/transfer? |
|---|---|---|---|---|---|---|
| 1 | Extraction of EHR data from Practice and hosting in secure cloud environment | HealthCare Provider EHR system | uMed | System… | Files are transferred using GPG encryption. Access control rights; password management protect the data once it has been anonymised and inserted into other databases. uMed has been certified to undertake this as part of the IM1 pairing process | UK based … |
| 2 | Engagement of relevant patients with study information | uMed | Patient | System… . | Access control rights; password management | UK based … |
| 3 | Electronic questionnaire data captured +/- consent from patient and held with hosted EHR data in secure cloud | Patient | uMed | System… . | Access control rights; password management | UK based … |
| 4 | Transfer of study specific data to external research organisation | uMed | Research Org | System… | **No transfer of data to external organisations takes place until the data controlled and data subject has consented, and study specific instructions provided to uMed for transfer<br><br>GPG encrypted files. Access control rights; password management | Reseach O… |

**Flow(s) Diagram**




**Flow Ref 1- Data Flow of uMed Platform**

**Section 4: Information Technology & Operations**

| 4a) System name | Used by e.g. organisation and dept. | Parties/system supplier |
|---|---|---|
| uMed Technology Platform | GP Practice, Patient | n/a |

*List any applicable electronic systems/software to this initiative (current and/or new):*

| 4b) Confirmation of IT involvement – IT lead(s)/support | | |
|---|---|---|
| **Name** | **Organisation** | **Involved Y/N** |
| Christopher Broderick | uMed | Y |
| Glen Swinfield | uMed | Y |

**4c) other assets:** ***Specify any other relevant assets relating to the personal data being processed either in use or intended***

| Asset name e.g. *child health record* | Format e.g. *paper/excel spreadsheet* | Asset id (linked to organisation Information asset register) – *if not yet registered leave blank* |
|---|---|---|
| n/a | | |

| 4d) | Where a data system is in use as part of the project/initiative confirm the following: | |
|---|---|---|
| i) | Staff access is vetted | Yes ☑ Explain process: All staff are vetted when first joining uMed, staff accessing PI will also have DBS checks.<br><br>HR03-Recruitment, Induction, Transfers, Changes and Leavers SOP[3]<br><br>HR04-Training and Competency[3]<br><br>No ☐ If no, explain: |
| ii) | Appropriate role-based access controls are in place for all staff who have access | Yes ☑<br><br>Explain process or embed relevant documentation:<br><br>IT10-Acceptable Use Policy[3]<br><br>No ☐ If no, explain: Click here to enter text. |
| iii) | An Information Asset Owner (IAO) and Information Asset Administrator (IAA) been assigned for the system | Yes (specify below) ☑<br><br>No ☐ Don't know ☐<br><br>IAO: Matt Wilson<br>IAA: Chris Broderick |

| 4e) | Any Other DPIA Appendix Specifics *(studies specific activities, study scope, etc as required)* |
|---|---|
| | Study specific documents will be provided for review via the uMed platform as each new study opportunity is identified. This may include a supplement to this DPIA if wider processing activity is required |

## **Section 5:** Information Technology Department **(to be completed by CTO or Head of Engineering)**

### a) Information governance project assurance

| GDPR Article 35(3) and ICO guidance 35(4) | | Yes | No | Unsure | Comments<br>*Document initial comments on the issue and the privacy impacts or clarification why it is not an issue* |
|---|---|---|---|---|---|
| i) | Is there to be **systematic and extensive profiling with significant effects**:<br>"(a) any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person" | ☐ | ☑ | ☐ | No systematic evaluation of data subjects is undertaken by the uMed platform. If a study requires further profiling of the data subject by uMed then this will be communicated to the data subject as part of the informed consent process |
| ii) | Is there **large-scale use of sensitive data**:<br>"(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10". | ☑ | ☐ | ☐ | The core processing activity provided by uMed results in no impact on privacy as no data is shared externally, and no activity takes place affecting the patient until the data controller (practice) has agreed to a specific study. At this point, consent will be sought for participation and the patient will be presented with information explaining how |

| GDPR Article 35(3) and ICO guidance 35(4) | | Yes | No | Unsure | Comments<br>*Document initial comments on the issue and the privacy impacts or clarification why it is not an issue* |
|---|---|---|---|---|---|
| | | | | | sensitive data may be used as part of a uMed supported study |
| iii) | Is there **monitoring of the public**:<br>"(c) a systematic monitoring of a publicly accessible area on a large scale" | ☐ | ☑ | ☐ | N/A |
| iv) | Does the processing involve the use of **new technologies**, or the novel application of existing technologies (including AI). | ☐ | ☑ | ☐ | uMed uses well established technologies including secure cloud hosting of data |
| v) | Is there any **denial of service**: Decisions about an individual's access to a product,<br>service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data | ☐ | ☑ | ☐ | N/A. |
| vi) | Does the initiative involve **profiling of individuals on a large scale**? | ☐ | ☑ | ☐ | N/A |
| vii) | Is there any processing of **biometric** data? | ☐ | ☑ | ☐ | N/A |
| viii) | Is there any processing of **genetic** data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject? | ☐ | ☑ | ☐ | N/A |
| ix) | Is there any **data matching**: combining, comparing or matching personal data obtained from multiple sources? | ☐ | ☑ | ☐ | N/A |
| x) | Is there any **invisible processing**: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort. | ☐ | ☑ | ☐ | N/A |
| xi) | Is there any **tracking** of individuals: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment. | ☐ | ☑ | ☐ | N/A |
| xii) | Is there any **targeting of children or other vulnerable individuals**: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children. | ☐ | ☑ | ☐ | N/A |
| xiii) | Is there any **risk of physical harm**: Where the processing is of such a nature that a<br>personal data breach could jeopardise the [physical] health or safety of individuals | ☐ | ☑ | ☐ | N/A |

**b) Processing Information Governance**

| | | | **Action required – ensure covered in section 6** |
|---|---|---|---|
| 5.1 | Are the arrangements for individual's to either ***object*** to their information being shared or to withdraw ***from the*** initiative for once they have been provided with appropriate guidance about it, appropriate? (See 1.4 – 1.6) | Yes ☑<br>No ☐ | Patients will be given guidance on consent. Choice will be respected and applied by either National opt-out or by not consenting to sharing data with a third-party study sponsor. |
| 5.2 | Confirm appropriate subject access handling/information rights procedures in place? | Yes ☑ No ☐ state reason if no<br>Not applicable ☐ | CL01-Consent Guide[3]<br>CL02-Managing Patient Data[3] |

| | | | **Action required – ensure covered in section 6** |
|---|---|---|---|
| 5.3 | Who are the controllers in this initiative? | Participating healthcare providers (i.e. GP Practices) | |
| 5.4 | Are there any other data processors and have the processors had oversight and opportunity to input into this DPIA? | Not applicable – no other processors ☑<br><br>Yes ☐ No ☐ Planned ☐<br><br>Don't know ☐ | |
| 5.5 | Are the contractual terms at 1.11 sufficient to satisfy compliance and information security? | Yes ☑ No ☐ Don't know ☐ | GEN12-uMed Platform User Terms and Condition[3]<br>GEN13-uMed Platform Data processing Agreement[3] |
| 5.6 | Is the information governance and information security training is in place and all staff with access to personal data have had up to date training | Yes ☑ No ☐<br>Don't know ☐ | DPA between uMed and GP's status of NHS Digital Security Toolkit. |
| 5.7 | Confirm appropriate measures in place to report incidents and share learning? | Yes ☑ No ☐<br>Don't know ☐ | IMS05-IS Breaches and Near Misses Policy and Log[3] |
| 5.8 | Does the processor of personal identifiable data a 'trusted' organisation e.g. completed a satisfactory Data Protection and Security Toolkit Assessment or other recognised standard? | Yes ☑ No ☐<br>Don't know ☐<br><br>If yes, enter details:<br>Link to DSP Toolkit . | |
| 5.9 | Is the processor registered with the ?<br><br>Information Commissioners - Data protection public register | Yes ☑<br>Registration No. and renewal date<br>ZA486572; 13 January 2023<br><br>No ☐ Don't know ☐ | |
| 5.10 | Lawful Basis for processing:<br><br>**Article 6:** Public task<br>**Article 9:** Explicit consent<br><br>National Data Opt out (The national data opt-out allows a patient to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment - for research and planning.) For more information see link here. | | |

**Section 6 – Privacy issues identified and risk analysis**

The risks raised will be transcripted to uMed's main risk register and treatment plan (IMS02_A).
Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular look at whether the processing could possibly contribute to:

- unauthorised access to data
- undesired modification of data
- disappearance of data
- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage

Risk Register

| Risk | Description | Risk Pre-mitigation | | | Mitigation | Risk | | | Measure accepted |
|---|---|---|---|---|---|---|---|---|---|
| | | Impact | Likelihood | Score | | Impact | Likelihood | Score | |
| 1 | Malicious action by external party to access sensitive pseudonymised health data from uMed system | 3 | 1 | 3 | Pseudonymised sensitive data is encrypted at rest and hosted in a certified AWS environment in line with or exceeding the standards set by NHS Digital. Penetration testing performed annually | 2 | 1 | 2 | Yes |
| 2 | Malicious action by external party to access personal data from uMed system | 4 | 1 | 4 | Personal data is encrypted at rest and hosted in a certified AWS environment in line with or exceeding the standards set by NHS Digital. Access control management implemented | 2 | 1 | 2 | Yes |
| 3 | Malicious action by external party to access identifiable sensitive data from uMed system | 4 | 1 | 4 | uMed uses a de-linked and encrypted identifier to connect pseudonymised and identifiable datasets which are held in separate AWS instances. The encryption key itself is held in a separate Key Management Service. Malicious actors would have to simultaneously gain access to multiple distinct AWS instances as well as the Encryption Key Service to attempt re-identification. This level of security far exceeds those standards set by NHS digital and many of the existing cloud hosted integrated care records | 2 | 1 | 2 | Yes |
| 4 | Malicious action by Umedeor employee to access, alter or exploit data held on uMed system | 4 | 1 | 4 | uMed has implemented SOPs to address this risk including confidential policy, password management, acceptable use policy, register and de-register starters and leavers access. Staff training and awareness. | 2 | 1 | 2 | Yes |
| 5 | Patients receive unwanted solicitation to engage in research | 1 | 3 | 3 | All correspondence makes clear to the subject why they are being contacted and how to change preferences to prevent unwanted further correspondence | 1 | 1 | 1 | Yes |
| 6 | A patient's health data is shared with a 3rd party organisation by a *practice* using uMed system against their expectations or wishes | 3 | 3 | 9 | This risk is not exclusive to uMed and exists for all current and future data sharing agreements (DSA) between *practices* & third parties. When using uMed patients associated with a specific DSA will be informed even when sharing does not require consent as a legal basis. This allows patients to 'opt-out' of a given DSA. | 3 | 1 | 3 | Yes |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 7 | A patient is misidentified in communications leading to preferences and / or responses being associated with another record | 3 | 3 | 9 | Patient identity will be confirmed before any legally binding consent is obtained. This is achieved by asking the patient to confirm DOB which is cross referenced with the DOB held against the record associated with the contact information in question. This contact information is obtained from the practice which supports another implicit layer of identity verification | 3 | 1 | 3 | Yes |
| 8 | A 3rd party research group (e.g. Pharma company) who access sensitive data via the uMed system utilises this data for purposes beyond those stated in the data sharing agreement. | 4 | 2 | 8 | If uMed is used to facilitate data sharing with a 3rd party, access is only granted once the data sharing agreement is in place. Audit logs give an immutable record of activity and any access by named individuals within a 3rd party. Like all DSAs, breach of this would result in legal action by the practice. | 4 | 1 | 4 | Yes |
| 9 | Patient preferences listed in uMed conflict with those held by the patient's healthcare provider or NHS digital. | 3 | 3 | 9 | uMed will flag any patients with preferences that conflict from those held on the NHS spine or are already coded within the patient record. uMed will default to declining 3rd party engagement until the discrepancy has been remedied | 3 | 1 | 3 | Yes |
| 10 | Umedeor Ltd fails to meet compliance requirement for information and security governance | 4 | 2 | 8 | uMed will always demonstrate compliance with the NHS Digital Data Security Protection Toolkit. uMed recognises the importance of IG and will address any deficit as a matter of urgency. Governance procedures, documentation and reports are available on request. uMed is ISO27001:2013 certified. | 4 | 1 | 4 | Yes |
| 11 | Umedeor Ltd becomes insolvent whilst holding sensitive data within the uMed system | 3 | 1 | 3 | In the unlikely event Umedeor Ltd becomes insolvent, all data created from patient engagement including metadata and logs will be returned to the data controllers associated with their patient population. All copies of sensitive and personal data will be destroyed and access granted to *practices* and / or independent auditors to demonstrate this. | 3 | 1 | 3 | Yes |

The following table should be used to decide upon the most appropriate likelihood for a particular threat.

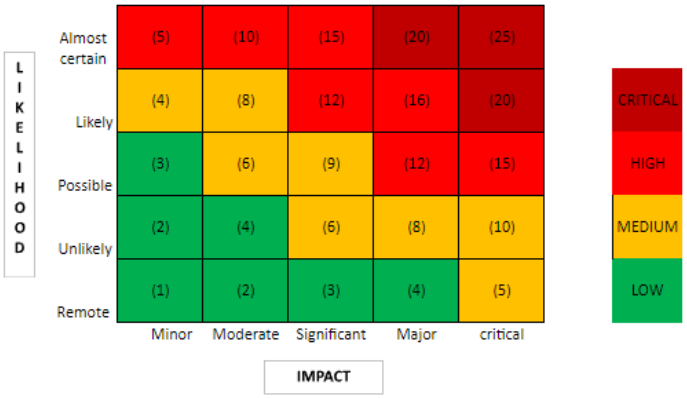
| Likelihood | Description | Summary |
|---|---|---|
| 1 | Remote | Has never happened before and there is no reason to think it is any more likely now |
| 2 | Unlikely | There is a possibility that it could happen, but it probably won't |
| 3 | Possible | On balance, the risk is more likely to happen than not |
| 4 | Likely | It would be a surprise if the risk did not occur either based on past frequency or current circumstances |
| 5 | Almost certain | Either already happens regularly or there is some reason to believe it is virtually imminent |

The following table should be used as guidance to help to decide upon the correct impact rating for a particular threat.

| Impact Level | | Impacted Areas | | | | |
|---|---|---|---|---|---|---|
| Impact Rating | General Description | Effect on Clients; projects | Financial Cost | Health and Safety | Damage to Reputation | Legal, contractual and organisational Compliance |
| 1 | Minor | Some local disturbance to normal business | Some | Within acceptable limits | Slight | Small risk of not meeting compliance |
| 2 | Moderate | Can still deliver product/service with | Unwelcome but could be borne | Elevated risk requiring immediate attention | Moderate | In definite danger of operating illegally |
| 3 | Significant | Some local disturbance to normal business operations | Severe effect on income and/or profit | Significant danger to life | Significant | Operating illegally in some areas |
| 4 | Major | Some areas of the business are out of | Major financial loss | Real or strong potential loss of life | Major | Fines and possible legal charges |
| 5 | Critical | Out of business; no service to customers | Crippling; the organisation will go out of business | Loss of life | Very High | Severe fines and possible imprisonment of staff |

## Classification of Risk Level

The chart below shows the rating scheme used to determine risk level based on a combination of likelihood and impact.



**Section 7 – Conclusion** (tick one of the following)

☐ All privacy risks have been identified and actions are underway to mitigate, accept or remove the risks. This action plan will now be reviewed and monitored in line with IMS02-Risk Management framework[3]

☑ All privacy risks have been identified and actions completed to mitigate, accept or remove the risks

*uMed Risk Assessment and Treatment Plan (IMS02_A)*

☐ Not all privacy risks can be removed or reduced and the processing remains high risk, therefore the ICO must be consulted

**Section 8: DPIA Approval and Sign off *(all involved stakeholders)***

Approved by:

| Department | Name | Date |
|---|---|---|
| uMed Management/DPO | Matt Wilson | 29/09/2022 |
| uMed Compliance | Teresa Latta | 29/09/2022 |
| uMed Operations | Abi Dhillon | 29/09/2022 |
| uMed IT/CTO | Chris Broderick | 29/09/2022 |
| Practice DPO | [Name] | [Date] |
| DPIA Populated Version | Date | Change |
| 2.2 | 29/09/2022 | Update supporting documentation links |

| Monitor and review of this DPIA | Who by:<br>Teresa Latta | When<br>29/11/2022 |
|---|---|---|