Data Protection Impact Assessment

For Receiving Diabetic Eye Screening (DES)

Patient Data via

MIQUEST-based Exports

Version 1.2

Date: 30th September 2019

# Introduction

This document must be completed for any new or change in service which pertains to the utilisation of personal identifiable information. It must be completed as soon as the new service or change is identified and in any event prior to go-live.

This process is a mandated requirement of the General Data Protection Regulation (GDPR) to ensure that privacy concerns have been considered and actioned to ensure the security and confidentiality of the personal identifiable information.

Privacy Law compliance checks and GDPR compliance checks are part of the DPIA process – the questions to assess this are included in the proforma.

The Project Lead should complete the documentation as they are closest to the detail of what is being proposed; where a Project Team exists, the Data PIA should also be reviewed by the Team.

Please complete all questions with as much detail as possible and return the completed from to Health Intelligence’s Data Protection Officer.

Further guidance on specific items can be found on the Information Commissioner’s website.

<https://ico.org.uk/>

# Section A: New/Change of System/Project General Details

|  |  |  |
| --- | --- | --- |
| Name: | Phil Kirby | |
| Objective/Purpose: | Securing the flow of patient data from General Practice in support of the Diabetic Eye Screening Programmes operated by Health Intelligence Ltd | |
| Background: | MIQUEST is a long standing solution that supports the export of patient data from General Practice. It was first introduced with the Requirements for Accreditation (RFA) 1999 and has been supported since its introduction. NHSX (formally NHS Digital) hold a contract with each GP Practice Clinical System supplier (EMIS, TPP, Vision, Microtest) (GP Systems of Choice) that requires MIQUEST to be supported.  Health Intelligence Ltd (HI) has actively used MIQUEST for almost two decades. Its supports the precise selection of both the cohort of patients of interest and the data set to be exported. Used correctly it is therefore the perfect tool to ensure that the agreed data set can be specified and obtained. | |
| Benefits: | MIQUEST enables the detailed specification of the data set to be exported and support the restriction of the cohort of patients to be exported. MIQUEST scripts can be loaded onto a Practice Clinical system and run to generate the required data export. Operated for Diabetic Eye Screening (DES) data flows on a monthly basis, we are able to maintain an accurate Single Collated Lists (SCL) a fundamental component of a high-quality Diabetic Eye Screening Programme. | |
| Constraints: | MIQUEST requires scripts to be run on the Practice Clinical System which therefore necessitates remote connection to initiate the MIQUEST scripts and then collate the output. This is only viable over N3/HSCN using a NHS accredited remote connection tool, “LogMeIn” or “Away from my Desk”.  When using the tool, the Practice user is telephoned and requested to connect to a website where they can then authorise the connection. A member of HI’s Support Services Team will then take control of the PC to initiate the export of data using MIQUEST scripts.  A Data Export Definitions (DED) document precisely defines the data set and the cohort of patients that the data set is provided for. A comprehensive testing regime ensure the MIQUEST scripts are kept in line with changes to the DED document as they occur. | |
| Relationships: | The GP Practice is the Data Controller and we have Data Sharing Agreements (DSAs) in place with each Practice.  Whilst HI is a Data Processor in the context of the data exported from General Practice the DSA does cover:   * The scope of the data to be exported and hosted (Schedule 1) * The organisations which the patient data will be shared with for direct patient care (Schedule 2) * The access to HI systems that is enabled for GP Practice users (Schedule 3). | |
| Quality expectations: | At least monthly based data exports from all participating GP Practices. | |
| Data Controller(s) | General Practice | |
| Data Processor(s) | Health Intelligence Ltd (HI) | |
| Cross reference to other projects: | None. | |
| Project Manager: | Name: | Adelaide Mitchell |
| Title: | DESP Co-ordinator |
| Department: | Support Services Department |
| Telephone: | 01270 527 373 |
| Email | Adelaide.Mitchell@health-intelligence.com |
| Information Asset Owner / Administrator:  (All systems/assets must have an Information Asset Owner (IAO) or Information Asset Administrator (IAA). IAO’s & IAA’s are normally the System Managers / Project Leads) | Name: | Chris Sagar |
| Title: | IT Manager |
| Department: | IT |
| Telephone: | 01270 765 124 |
| Email | chris.sagar@health-intelligence.com |
| Information Risk Owner:  (All systems / assets must have an Information Risk Owner (IRO) who is responsible to identifying and mitigating any risks to the Information Asset. IRO‟s are normally Heads of Departments and report to the SIRO) | Name: | Phil Kirby |
| Title: | Managing Director |
| Department: | Corporate |
| Telephone: | 07770 570117 |
| Email | phil.kirby@health-intelligence.com |

# Section B – Data Protection Impact Assessment Key Questions

|  |  |
| --- | --- |
| 1. Will the system/project/process (will now be referred to thereafter as ‘asset’) contain Personal Data and Special Categories Data? (Please reference Appendix 4)  If answered ‘No’ you do not need to complete any further information as DPIA is not required. | 🞎 Yes X  🞎 No |
| 2. Please state purpose for the collection of the data: for example, patient treatment, health administration, research, audit, staff administration | Provision of the Diabetic Eye Screening Programme (DESP). The DESP is a national initiative and involves the delivery direct patient care for patients with a diagnosis of diabetes aged 12 years and older. |
| 3. Does the asset involve new privacy–invasive technologies? | 🞎 Yes  🞎 No X  🞎 n/a  If yes, please give details: |
| 4. Please state the data items that are held in the system | Personal:  🞎 Name X  🞎 Address X  🞎 Date of Birth X  🞎 Gender X  🞎 NHS No. X  🞎 Other local identifier  🞎 GP Practice X  🞎 Consultant  🞎 Third Party Relationships  Sensitive:  🞎 Treatment dates X  🞎 Diagnosis X  🞎 Medical history X  🞎 Religion  🞎 Ethnic Group X  Other (please state here):  Examination Data X  Laboratory Test Results X |
| 5. Will the asset collect new personal data items which have not been collected before? | 🞎 Yes  🞎 No X (solution in use for almost two decades)  🞎 n/a  If yes, please give details: |
| 6. What checks have been made regarding the adequacy, relevance and necessity for the collection of personal and/or sensitive data for this asset? | A Data Minimisation Exercise took place during July & August of 2018. The Data Export Definitions document defines the data set and this is kept under regular review. |
| 7. Does the asset involve new or changed data collection policies that may be unclear or intrusive? | 🞎 Yes  🞎 No X  🞎 n/a  If yes, please give details: |
| 8. Are third-party contracts/suppliers being used?  For each specify details and reference any related Data Protection Impact Assessments | 🞎 Yes X  🞎 No  🞎 n/a  If yes:  Organisation Name: Health Intelligence Ltd  ICO Registration Number:  **Z845073X** End date: 18 February 2020  MIQUEST is a tool provided by the GP Practice clinical systems suppliers – so MIQUEST is not regarded as a third party – but perhaps the GP Practice Clinical System provider should be as they host the patient data on behalf of the GP Practice. |
| 9. Does the third party/supplier contracts contain all the necessary Information Governance clauses including information about Data Protection, Confidentiality, Staff Training, Subject Access Requests and Freedom of Information? | 🞎 Yes X  🞎 No  🞎 n/a  The Commissioners of the service is the NHS England & NHS Improvement - South East who within its tender processes have assessed IG, IT and security. Provisions are also included within the Data Sharing Agreement.  If no, please review contract details. |
| 10. Does the purpose of this information asset / project / process comply with GDPR and other privacy laws such as the Privacy and Electronic Communications Regulations 2003. | 🞎 Yes X  🞎 No  If No, please specify why: |
| 11. Who provides the data/information for the asset? | 🞎 General Practice X  🞎 Patient  🞎 Staff  🞎 Other – please specify:  🞎 n/a |
| 12. Are you relying on individuals (patients/staff) to provide consent for the processing of personal data and special categories data? | 🞎 Yes  🞎 No (please fill in Section C) X  🞎 n/a  If yes, please give details how will consent be obtained: |
| 13. Have the individuals been informed of all the processing and have given their consent to all the processing and disclosures? | 🞎 Yes (explicit)  🞎 Yes (implicit in leaflets, on website) X  🞎 Other – please specify:  🞎 No  🞎 n/a  If Yes – please give details and reference related documentation.  All Programmes has a Privacy Notice provided on their websites. Patients are directed to this when they attend for screening and also via Posters on GP Practice notice board.  The current Privacy Notce can be found here : <http://www.kmdesp.co.uk/diabetic-eye-screening/privacy-notice/> |
| 14. Does the system support patient/other data subject a) rectification, b) Right of access to person data c) the ability to restrict processing and d) the choice to opt out? | For each specify:  🞎 Yes  🞎 No  🞎 n/a X  If yes, please give details:  As the Data Controller, the GP Practice will address these requirements in their management of individual rights for their patients (access, rectification, erasure and restricting processing etc). This section is noted as “n/a” as the MIQUEST process only enables the export of filtered data from the GP Practice Clinical Systems.  Also see response to Q22.  If no, explain the situation: |
| 15. How will the information be kept up to date and checked for accuracy and completeness? | This initiative is about ensuring the Programme’s Single Collated List (SCL) is accurate and complete. Monthly MIQUEST data exports are undertaken for all GP Practices who sign the DSA and the output of the MIQUEST scripts are then automatically loaded using HI’s Export Transform and Load (ETL) system into the Single Collated List. |
| 16. Who will have access to the information? | All users with access to HI Hub and specifically the Spectra Programme Management (PM) module that maintains the SCL. |
| 17. Do you intend to send direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)? | 🞎 Yes  🞎 No X  🞎 n/a  If yes, please give details: |
| 18. If applicable, are there procedures in place for an individual’s request to prevent processing for purposes of direct marketing in place? | 🞎 Yes  🞎 No  🞎 n/a X  If yes, please give details: |
| 19. Is automated decision making (profiling) being used? | 🞎 Yes  🞎 No X  🞎 n/a  If yes, please give details: |
| 20. Is there a useable audit trail in place for the asset? For example, to identify who has accessed a record? | 🞎 Yes X In terms of both the ETL and HI Hub  🞎 No  🞎 n/a  If yes, please give details:  The ETL records what data has been presented to HI Hub to load and HI Hub’s audit logging functionality supports the audit of all access. |
| 21. Have you assessed that the processing of personal/sensitive data will not cause any unwarranted damage or distress to the individuals concerned? | 🞎 Yes X  🞎 No  🞎 n/a  If yes, please give details:  The flow of data is to ensure patients are not missed from being offered diabetic eye screening and protecting their eyesight. |
| 22. What procedures are in place for the rectifying/blocking of data by individual request or court order? | Health Intelligence’s Data Protection Officer (DPO) will manage all such requests (as they are likely to be directed to the provider of the Programme). The Practice will be involved as required. If the individual wishes to request that their data is corrected, we will ensure the correct is applied on the Programme register and the Practice is requested to correct their clinical system also. An example: a patient is referred by the Practice to the Programme, we invite the patient, but the patient then disputes that they are diabetic. Health Intelligence would check with the Practice and if the Practice confirmed this position, the patient record would be corrected on both the Programme Register and the Practice Register.  Health Intelligence undertakes a formal DPO mailbox and assessment process weekly with the DPO and Caldicott Guardian to ensure all such request can be managed in a timely manner. |
| 23. Does the asset involve new or changed data access or disclosure arrangements that may be unclear? | 🞎 Yes  🞎 No X  🞎 n/a  If yes, please give details: |
| 24. Does the asset involve changing the medium for disclosure for publicly available information in such a way that data become more readily accessible than before? (For example, from paper to electronic via the web?) | 🞎 Yes  🞎 No X  🞎 n/a  If yes, please give details: |
| 25. What are the retention periods (what is the minimum timescale) for this data? (please refer to the Records Management: NHS Code of Practice) | The retention period for the data stored within the MIQUEST and related Export Transform & Load system is three months. This period is sufficient to address any queries with the MIQUEST based data export process. |
| 26. How will the data be destroyed when it is no longer required? | The data will be deleted from the server and all cycled backup copies. |
| 27. Will the information be shared with any other establishments/ organisations /Trusts? | 🞎 Yes X  🞎 No  🞎 n/a  If yes, please give details:  Yes, however only once loaded into HI Hub (Spectra PM) in line with the Data Sharing Agreements (Schedule 2 of the embedded Data Sharing Agreement) signed with each GP Practice. By signing the DPA, the Practice is confirming that patient data may be shared with other relevant organisations who are providing direct patient care services. For example, we will facilitate the provision of information to the Ophthalmology Department in support of a referral from the Programme. |
| 28. Does the asset involve multiple organisations whether public or private sector?  Include any external organisations. Also include how the data will be sent/accessed and secured.  Provide reference to a data flow diagram showing the flows of data between organisations. | 🞎 Yes  🞎 No X  🞎 n/a  If yes, please give details: |
| 29. Does the asset involve new linkage of personal data with data in other collections, or are there significant changes in data linkages? | 🞎 Yes  🞎 No X  🞎 n/a  If yes, please give details: |
| 30. Where will the information be kept/ stored/ accessed? | The Project is concerned with the flow of patient data from the GP Practice clinical system, using MIQUEST to HI’s ETL system for loading into HI Hub.  The data will be temporarily stored in the ETL – cleared down quarterly. The data will be kept within HI Hub for the duration of the DESP contract. |
| 31. Will any information be sent off site? | 🞎 Yes  🞎 No X  🞎 n/a  If yes, please give details including method of transportation: |
| 32. Are you transferring any personal and / or sensitive data to a country outside the European Economic Area (EEA)? | 🞎 Yes  🞎 No X  🞎 n/a  If yes, please give details of where: |
| 33. Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country? | 🞎 Yes  🞎 No  🞎 n/a X  If yes, please give details: |
| 34. Have you checked that the non-EEA country has an adequate level of protection for data security? | 🞎 Yes  🞎 No  🞎 n/a X  If yes, please give details: |
| 35. Is there a Security Management Policy and Access Policy in place? Please state policy titles. | 🞎 Yes X  🞎 No  🞎 n/a  If yes, please state policy titles:  HI employees confirm their agreement to our Security Policy. HI’s Access Control Policy ensures that all users are only given appropriate access to systems. |
| 36. Has an information risk assessment been carried out and reported to the Information Asset Owner (IAO)?  Where any risks highlighted and how these will be mitigated? – please provide details | 🞎 Yes X  🞎 No  🞎 n/a  If yes, please give details:  See section E. |
| 37. Is there a contingency plan / backup policy in place to manage the effect of an unforeseen event? | 🞎 Yes X  🞎 No  🞎 n/a  If yes, please give details:  If the data does not flow via MIQUEST, then HI can obtain the data via the GP Practice’s own reporting suite or via GP2DRS.  GP2DRS will be deployed during 2019 as a backup and contingency measure. |
| 38. Are there procedures in place to recover data (both electronic /paper) which may be damaged through:  • Human error  • Computer virus  • Network failure  • Theft  • Fire  • Flood  • Other disaster  Please reference relevant policies. | All data exported out of the GP Practice clinical system is clearly still present within the GP Practice clinical system and could therefore be re-exported. |
| 39. Is the DPIA approved?  If not, please state the reasons why and the action plan put in place to ensure the DPIA can be approved | Yes |

# Section C – Compliance with the General Data Protection Regulation Articles 6 & 9 for Processing

|  |  |  |  |
| --- | --- | --- | --- |
| **Article 6 – Lawfulness of Processing** |  | **Article 9 - Processing of special categories of personal data** |  |
| 1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes; | 🞎 | 1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; | 🞎 |
| 1. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; | 🞎 | 1. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; | 🞎 |
| 1. processing is necessary for compliance with a legal obligation to which the controller is subject; | 🞎 | 1. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; | 🞎 |
| 1. processing is necessary in order to protect the vital interests of the data subject or of another natural person; | 🞎 | 1. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; | 🞎 |
| 1. 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; | 🞎X | 1. processing relates to personal data which are manifestly made public by the data subject; | 🞎 |
| 1. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. | 🞎 | 1. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; | 🞎 |
|  |  | 1. processing is necessary for reasons of substantial public interest, on the basis of   Union or Member State law which shall be proportionate to the aim pursued, respect  the essence of the right to data protection and provide for suitable and specific  measures to safeguard the fundamental rights and the interests of the data subject; | 🞎 |
|  |  | 1. processing is necessary for the purposes of preventive or occupational medicine, for   the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional | 🞎X |
|  |  | 1. 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 quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; | 🞎 |
|  |  | 1. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject | 🞎 |

# Section D – Data Flow Map

(Please indicate where security controls are in place)

|  |  |  |
| --- | --- | --- |
|  | **GP Practice Clinical System – Data is Exported via MIQUEST Scripts** |  |
|  |  |  |
|  | **Transferred Encrypted over N3/HSCN using remote “LogMeIn” or “Away from my Desk”** |  |
|  |  |  |
|  | **Loaded into HI’s Extract Transform & Load (ETL)** |  |
|  |  |  |
|  | **Loaded into HI’s HI Hub system and into the Spectra PM module (SCL)** |  |

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

1. Identify the privacy and related risks (see Appendix 1 for further information)

*Note. By allocating a reference number to each identified privacy issue will ensure you link back to this throughout the rest of the assessment. Column (a), (b) and/or (c) must be completed for each privacy issue identified in column*

| **Ref No.** | **Privacy issue –** element of the initiative that gives rise to the risk | 1. **Risk to individuals** *(complete if appropriate to issue or put not applicable)* | 1. **Compliance risk**   *(complete if appropriate to issue or put not applicable)* | 1. **Associated organisation/corporate risk** *(complete if appropriate to issue or put not applicable)* |
| --- | --- | --- | --- | --- |
| *Example: PR1* | *Individuals are not aware of the initiative as no communication materials have been planned* | *Individuals not aware that their data is being processed* | *Non-compliance with GDPR Article 6 – Lawfulness of Processing* | 1. *May lead to public mistrust* 2. *May lead to sanction by the Information Commissioners office (ICO)* |
| **PR1** | **The diabetes data set output from MIQUEST scripts does not match the Data Export Definitions (DED) document and not all records are exported** | **A delayed referral to the DESP**  **A delayed update to their administrative data (contained due to weekly PDS)** | **n/a** | **Screening Incident could be declared where referrals have been significantly delayed** |
| **PR2** | **The diabetes data set output from MIQUEST scripts does not match the Data Export Definitions document and additional records are exported** | **n/a** | **Breach of patient confidentiality (data processed outside of DSA) “Trusted Partner Breach”**  **Potential internal user disclosure** | **Potential for a Data Breach and reporting to the DPO** |
| **PR3** | **Unavailability of support for MIQUEST (support for MIQUEST may be withdrawn)** | **A delayed referral to the DESP**  **A delayed update to their administrative data (contained due to weekly PDS)** | **n/a** | **Potential for Data Unavailability and reporting to the DPO** |
| **PR4** | **GP Practices may not brief patients that they would be invited for Screening** | **n/a** | **Awareness of Data Processing** | **May receive complaints regarding the lack of transparency re data processing** |
| **PR5** | **Support Services staff my run the wrong version of the MIQUEST Scripts** |  | **This may inadvertently export more data that required in breach of the DSA** | **Potential for a Data Breach and reporting to the DPO** |

(Table 1)

1. Identify the privacy solutions

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Ref No.** | **Risk – taken from column (a), (b) and/or (c) in table 1.** | **Risk score – see tables at Appendix 2** | | | **Proposed solution(s)**  **/mitigating action(s)** | **Result:** is the risk accepted, eliminated, or reduced? | **Risk to individuals is now OK?**  **Signed off by?** |
| **Likelihood** | **Impact** | **RAG status** |  |  |  |
| *Example: PR1* | *Individuals not aware that their data is being processed*  *Non-compliance with GDPR Article 6 – Lawfulness of Processing*  *1. May lead to public mistrust*  *2. May lead to sanction by the Information Commissioners office (ICO)* | 5 | 5 | Red | *Communication plan to be developed to ensure compliance with fair and lawful processing*  *Assurance that there will be an active communication campaign*  *All relevant staff informed of need to understand and disseminate communication material.* | *Reduced to an acceptable level (it is not possible to eliminate at this stage as the Comms plan will need to ensure it addresses all aspects to enable individuals to be fully informed.* | *Yes*  *Sign-of tbc* |
| **PR1** | **The diabetes data set output from MIQUEST scripts does not match the Data Export Definitions (DED) document and not all records are exported** | **2** | **3** | **Amber** | **MIQUEST Scripts reviewed to ensure they match the DED document. Repeat validation checks with each update.** | **Reduced likelihood to 1** | **Yes** |
| **PR2** | **The diabetes data set output from MIQUEST scripts does not match the Data Export Definitions document and additional records are exported** | **2** | **4** | **Amber** | **MIQUEST Scripts reviewed to ensure they match the DED document. Repeat validation checks with each update.** | **Reduced likelihood to 1** | **Yes** |
| **PR3** | **Unavailability of support for MIQUEST (support for MIQUEST may be withdrawn)** | **5** | **5** | **Red** | **Prompt at national level the need to retain MIQUEST support (until another viable GDPR compliant solution operational)** | **Reduced Likelihood to 4** | **Yes, have to live with this risk. Viable alternatives in place as a backup and contingency option** |
| **PR4** | **GP Practices may not brief patients that they would be invited for Screening** | **2** | **3** | **Amber** | **Provide GP Practice Briefing Papers, Posters for display and Training** | **Given number of GP Practices difficult to reduce likelihood of occurrence** | **Yes** |
| **PR5** | **Support Services staff my run the wrong version of the MIQUEST Scripts** | **2** | **3** | **Amber** | **Only the current version of the MIQUEST scripts available to Support Service Personnel (also as a backup a check brick is used to prevent the wrong version of the MIQUEST script output being loaded)** | **Reduced Likelihood to 1** | **Yes** |

(Table 2)

1. Integrate the DPIA outcomes back into the project plan

*Note. This must include any actions identified in Table 1 and Table 2.*

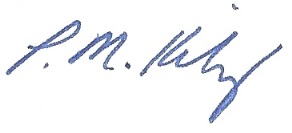
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Who is responsible for integrating the DPIA outcomes back in to the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?** | | | | | | | | |
| **Ref No.** | **Action to be taken** | **Date for completion of actions** | **Anticipated risk score following mitigation** | | | **Responsibility for action – *job title not names*** | **Current status/progress** |
| **Likelihood** | **Impact** | **RAG status** |
| *Example: PR1* | *Communications plan to be developed* |  | *2* | *2* | Green | *Project Manager to liaise with Communication lead and embed into project plan* | *Meeting arranged with Communication Lead* |
| **PR1 &**  **PR2 &**  **PR5** | **MIQUEST Scripts to be quality assured and verified against the latest version of the Data Export Definitions (DED) document.** | **May 2019** | **1** | **3** | **Amber** | **Head of Support Services, management overview by Managing Director** | **Last Review completed May 2019 (minor changes to scripts implemented and tested)** |
| **PR3** | **Continue to Promote MIQUEST as a valuable tool to be retained with DoH, NHSX, NHS England & NHS Improvement** | **Ongoing** | **4** | **5** | **Red** | **Managing Director** | **Meetings scheduled with BMA, LMCs and NHSX** |
| **PR4** | **Prompt transparency regarding data processing in support of direct patient care for DESP – Briefing Papers, Privacy Notices, Posters, Advice and Training for GP Practices** | **All material available and dispatched, hosted on the Programme’s website.**  **Practice training ongoing during April – September 2019 as Practices signup to the DSA** | **2** | **3** | **Amber** | **Marketing Manager**  **Support Service Department** | **All materials available.**  **Training underway** |

**Section F – Sign Off**

**Form completed by:**

Name: Phil Kirby

Title: Managing Director / Caldicott Guardian

Signature: 

Date: 22/05/2019

**Data Protection Officer Approval:**

Name: Michael Pennington

Title: Head of Operations and Security / DPO

Signature: 

Date: 23/05/2019

**Appendix 1: Types of Privacy Risks**

**Risks to individuals**

* Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
* The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people’s knowledge.
* New surveillance methods may be an unjustified intrusion on their privacy.
* Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
* The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
* Identifiers might be collected and linked which prevent people from using a service anonymously.
* Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
* Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
* Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
* If a retention period is not established information might be used for longer than necessary.

**Compliance risk**

* Non-compliance with the common law duty of confidentiality
* Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015
* Non-compliance with the GDPR.
* Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
* Non-compliance with sector specific legislation or standards.
* Non-compliance with human rights legislation.

**Associated organisation/corporate risk**

* Non-compliance with the Data Protection Legislation can lead to sanctions, fines and reputational damage.
* Problems which are only identified after the project has launched are more likely to require expensive fixes.
* The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
* Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, is less useful to the business.
* Public distrust about how information is used can damage an organisation’s reputation and lead to loss of business.
* Data losses which damage individuals could lead to claims for compensation.

**Appendix 2: Guidance for Completing a Risk Register**

* What is the actual risk? Make sure the risk is clear and concise and articulated with appropriate use of language, suitable for the public domain.
* Be careful and sensitive about the wording of the risk as risk registers are subject to the Freedom of Information (FOI) requests
* Don’t reference blame to other organisations in the risk register (the register may be made available in the public domain)
* Does the risk belong to a business area within your organisation or another body?
* It is common to use a RAG matrix rating system for assessing risk. RAG stands for red, amber, green. To achieve a RAG rating, each risk first needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

**Likelihood**

Likelihood Score 1 to 5 

**Impact**

Impact Score 1 to 5

Using the risk “RAG” rating system for scoring risks means risks can be ranked so that the most severe are addressed first. Decisions can then be made as to what mitigating action can be taken to alleviate the risk.

A

A/R

R

R

R

A

A

A/R

R

R

A/G

A

A

A/R

A/R

Very High -5

High - 4

Medium - 3

G

A/G

A/G

A

A

G

G

G

G

G

1

Rare

2

Unlikely

3

Possible

4

Likely

5

Almost Certain

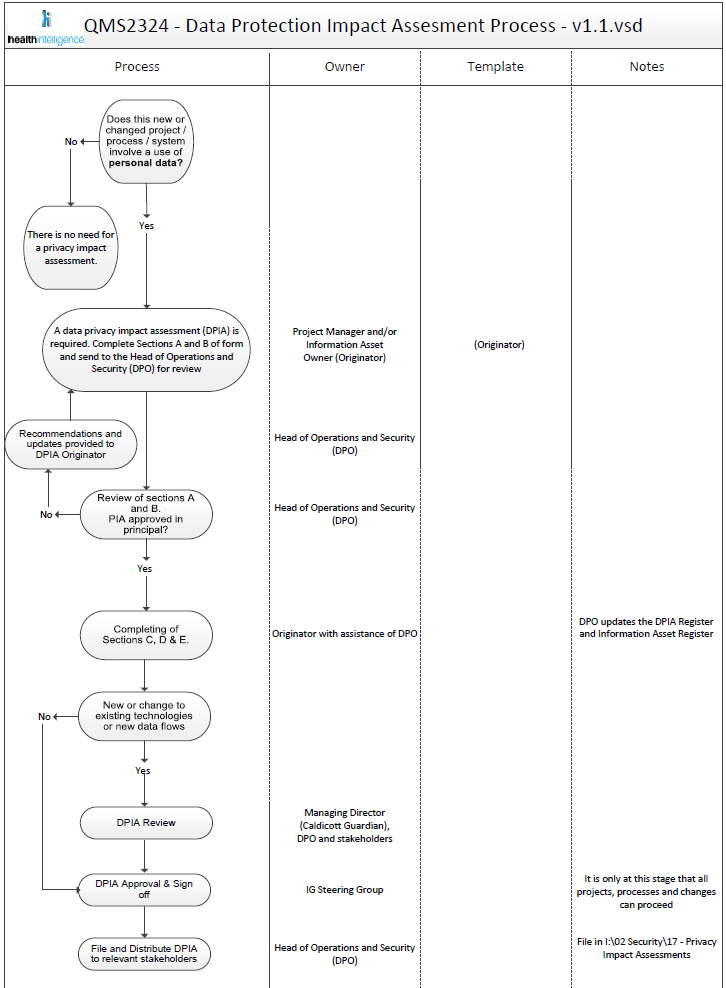
**Likelihood**

Low - 2

Very Low - 1

**Impact**

**Appendix 3 – Data Protection Impact Assessment Process Flowchart**

****

**Appendix 4 – Glossary of Terms**

|  |  |
| --- | --- |
| **Item** | **Definition** |
| **Personal data** | Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.  There is a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.  The definition applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.  Note: Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual. |
| **Special Categories data** | Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation |
| **Direct marketing** | This is "junk mail" which is directed to individuals. The mail which is addressed to "the occupier" is not directed to an individual and is therefore not direct marketing.  Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you.  Direct marketing does not just refer to selling products or services to individuals, it also includes promoting views or campaigns such as those of a political party or charity. |
| **Automated decision making** | Automated decisions only arise if 2 requirements are met. First, the decision must be taken using personal information solely by automatic means. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second requirement is that the decision has to have a significant effect on the individual concerned. |
| **European Economic Area (EEA)** | The European Economic Area comprises of the EU member states plus Iceland, Liechtenstein and Norway |
| **Information assets** | Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities.  Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware. |
| **Caldicott Guardian** | A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.  Caldicott Guardians were mandated for NHS organisations by Health Service Circular HSC 1999/012 and later for social care by Local Authority |
| **SIRO (Senior Information Risk Owner)** | This person is an executive who takes ownership of the organisation's information risk policy and acts as an advocate for information risk on the Board |
| **IAO (Information Asset Owner)** | These are senior individuals involved in running the relevant service / department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control / area. |
| **IAA**  **(Information Asset Administrator)** | There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers |
| **Implied consent** | Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure. |
| **Explicit consent** | Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patient's case notes) or in writing, to a particular use of disclosure of information. |
| **Anonymity** | Information may be used more freely if the subject of the information is not identifiable in any way - this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients. |
| **Pseudonymity** | This is also sometimes known as reversible anonymisation. Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference. |
| **Information Risk** | An identified risk to any information asset that the Organisation holds. Please see the Information Risk Policy for further information. |
| **Privacy Invasive Technologies** | Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk |
| **Authentication requirements** | An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks. |
| **Retention Periods** | Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives. |
| **Records Management: NHS Code of Practice** | This is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains-an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.  . |
| **General Data Protection Regulation (GDPR)** | Under the GDPR, the data protection principles set out the main responsibilities for organisations.  Article 5 of the GDPR requires that personal data shall be:   1. processed lawfully, fairly and in a transparent manner in relation to individuals; 2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; 3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; 4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; 5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and 6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.   Article 5(2) requires that:  the controller shall be responsible for, and be able to demonstrate, compliance with the principles |
| **Privacy and Electronic Communications Regulations**  **2003** | These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information. |

**Control Sheet**

Version 1.1 dated 14th June 2019 has had updates applied to Q8, Q9, Q14, Q22 and Q27.

Version 1.2 dated 30th September 2019 had updates to Q9 in terms of the Commissioners name, to Q13 now uses a URL instead of a embedded document for the Privacy Policy and Q27 (Data Sharing Agreement) is now customer specific, in this case for Kent and Medway.