Data Protection Impact Assessment: product deployment

1. Introduction

This Data Protection Impact Assessment has been produced by QMasters to assess the Data Protection Risk of the deployment of its products into EMIS clinical systems. It concludes that no significant Information Governance risk is created by these processes; Practices are informed of a low residual risk and advised of mitigating actions.

This assessment is undertaken annually and in response to newly-identified risks.

2. Product description

Data validation

- Our Summary Report offers an overview of the number of patients with coding errors and their value in terms of unclaimed QOF income.
- Our Detailed Report contains EMIS ID, Usual GP, and the clinical code that needs adding/changing for each individual patient. It includes instructions explaining how to easily replace the incorrect clinical code with the correct one.

QToolset Enterprise

- QToolset Enterprise offers clear, concise, and intuitive templates that automatically adapt for individual patients based on the data within their clinical record. It includes templates for long-term conditions, QOF, enhanced services, frailty, and many other clinical areas. The templates are customised to incorporate local guidelines, websites, and patient information leaflets.

3. Data

The data processed by QMasters is not Person Identifiable Data or PID. The only identifier is the EMIS number; thus the only personnel able to identify the patient are those employed by the Practice.

4. Deployment mechanisms

- These are described in the attached process maps
- Deployment requires that QMasters associates are granted access to the Practice EMIS system, as detailed in the Terms and Conditions section 8.5 and section 9.
    - The recommended RBAC codes, *B0994 (Manage ad-hoc reports (local))* and *B1700 (Local System Configuration)* do not allow the user to view the clinical record. However, it is possible at this stage for QMasters associates to access Personal Identifiable Data. This is described in more detail in *Section 8: Risk Assessment*, below

5. Compliance with Caldicott principles

No.	Principle	Compliance
1	**Justify the purpose(s)** Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.	Direct patient care and its administration: the actual delivery of care by healthcare professionals and the necessary administrative and support functions to ensure safe and effective delivery and proper communication between those involved
2	**Don't use personal confidential data unless it is absolutely necessary** Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).	Personal confidential data is not used
3	**Use the minimum necessary personal confidential data** Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.	Personal confidential data is not used
4	**Access to personal confidential data should be on a strict need-to-know basis** Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.	Access to personal confidential data is restricted by RBAC codes
5	**Everyone with access to personal confidential data should be aware of their responsibilities** Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.	All QMasters associates receive and understand the required level of IG training
6	**Comply with the law** Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.	Although it has been demonstrated that Personal Confidential Data is not being used by QMasters, the purpose of QMasters products is: • The provision of health or social care • The management of health or social care systems As provided for in Article 9 (2) (h) in the GDPR

7	**The duty to share information can be as important as the duty to protect patient confidentiality** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.	Not applicable

6. Data retention and disposal

De-identified data will be stored securely on Google Drive Professional in Europe by QMasters for between one and two years following the end of the contract

7. Transparency

It is recommended that the Practice makes reference to the use of de-identified data by 3rd parties to improve data quality in Data Privacy Notices and other forms of communications, and makes available the relevant information about QMasters processes on request

8. Risk assessment

Personal data is neither accessed nor stored by QMasters. A small residual risk remains, as mentioned above, and described in the table below

QMasters deployment risk	
Hazard	QMasters associates are able to access Personal Identifiable Details of patients whose data is used in the report
Cause	The RBAC codes necessary for deployment do not restrict this level of access
Existing safeguards	Professional accountability of QMasters associates
Consequences	Minor/ moderate
Likelihood	Unlikely
Overall risk rating	Low
Mitigation	This cannot be mitigated any further by QMasters. Practices may, if they wish, run reports to verify the data accessed by QMasters

9. Review

Date	Version	Produced by	Detail
09/07/18	1.0	Merlin Dunlop / Maggie Lay	First DPIA