Attachment H – Unsighted (black box) processing

There are a number of points in relation to the processing of the data to support analytical activities. The aim of the processing is to produce three distinct views of the data that support different activities. These views are described as 'data marts' in the Graphnet model and include the following:

- ***Fully identifiable data mart*** – to be used for case finding and direct patient care decision support by clinical users and primary care staff
- ***Fully anonymised data mart*** – to be used for population heath management, risk stratification and monitoring of intervention outcomes by Public Health, analysts, managers and admin staff.
- ***Pseudonymised data mart*** – to be used for population heath management, risk stratification and monitoring of intervention outcomes by Commissioners, CCG analysts and service managers. Whilst preventing these staff from seeing identifiable data, the pseudonymised data mart allows those staff where needed to liaise with staff providing direct care about the same individual where required, i.e. if 10 pseudonymised patients are identified in an analysis the pseudonyms can be shared with those with access to the identifiable data mart where they can fully identify the patient and provide a direct care intervention.

Access to the datamarts is determined by Role Based Access controls.

There are a number of processes being undertaken by Graphnet to move from the Care Centric platform for direct care to the three 'data marts' supporting analytical activities.

There is a need to take a copy of the live Care Centric record into the Azure Data Factory, so that any of the processing work does not affect the provision of the platform for direct care support.

The output is then accessed through the three data marts identified above.

GMC guidance on 'the process to anonymise information' is presented in Attachment G.

The processing by Graphnet must either not present the risk of breaching confidentiality or must have an appropriate legal basis to meet the requirements of the common law of confidentiality.

We have requested and received further reassurance from Graphnet that the processes described above are all conducted as 'automated processing'. No member of staff from Graphnet is involved in manual processing of identifiable data. They state:

> *'These processes are fully automated using Azure data factory and Azure SQL Server Integration services. No human sees data during these processes unless in direct response to a customer raised support call which requires investigation at a data level.'*

The automated processes, up to the point of production of the three data marts in the diagram do not result in a disclosure of confidential information to an individual as no person is involved in these activities.

Section 79 in the GMC guidance requires there to be a disclosure for the common law of confidentiality to be engaged. The processes to develop the anonymised data mart and the pseudonymised data mart do not result in a disclosure.

It is agreed that the CAG approval for risk stratification only covers part of the processing in relation to risk stratification. Which means that, CAG approval does not cover all the processing purposes and therefore it is not relied upon to meet common law requirements.