**Pseudonymisation Audit**

Following the meeting which was help on the 17th December 2018, I have complied the following from the discussions around what would constitute a pseudonymisation audit.

Trusts should have or are actively mapping flows of data as part of Data Flow Mapping Exercise’s and creating Asset Registers as a requirement of preparedness for the GDPR and DP regulation.

These exercises at will identify the which flows are,

**Full PID** – personal data

**De-Identified/anonymised** – the process of turning data into a form which does not identify individuals and where identification is not likely to take place, resulting in data that is, therefore, not personal.

**Pseudonymisation**– a security measure organisations can apply to personal data, much like encryption. The GDPR explains that pseudonymisation, is the processing of personal data in such a way that the data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.

For the purpose of Data Security Standard 1.

* Date of last audit of pseudonymisation, anonymisation or de-identification controls
* Overall findings of last audit of [pseudonymisation, anonymisation or de-identification] controls.

**Re-evaluate your flows – (Audit)**

* Are the flows identified still required or have they been superseded.
* If the flows are still required are they still adequate for the requirement (is the data relevant and not excessive (PID))
* In line with Data Protection Legislation ascertain if there is an identified legal basis for sharing the information review if the existing flows are still categorised correctly and the legal basis is correct.
* Does the flow still need to remain Full PID, De-Identified, Pseudonymised or anonymised
* If a flow of pseudonymised data is identified, has the flow been reviewed and assurance obtained that keys are held separately and the technical solution of the share reviewed to ensure secure.

Do you have a Pseudonymisation Policy or policy which reflects the expectations required from the Data Protection Legislation and DSPT.