How can Aridhia's De-identification Service help client compliance?

De-Identification Service Product features	High Level Compliance Requirements			
	Data Protection Act 1998	**Caldicott Principles**	**NHS England IG Toolkit**	**EU DP Directive**
De-Identifying the same identifier in two different projects will produce different de-identified values. This ensures that researchers cannot compare or cross-link datasets between separate projects.	Principle 7 Appropriate technical and organisational measure shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	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). 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. 4. Access to patient-identifiable information should be on a strict need-to-know basis Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.	CCG`s - 12-352 & CSU and Acute Trust- 12-324 The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate	Article 6 principles relating to data quality e.g. Article 6 1 (e): The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Article 17 – Security of Processing the controller must implement appropriate measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access;
Provides 14 core anonymisation plug-ins as default.				
Provides ability to create and implement own de-identification algorithms.				
Supports a re-identification protocol that can be followed in specific circumstances e.g. patient safety reason to enable (only) the data controller to identify a pseudonymised patient.				
Allows de-Identification of the same identifier to produce a consistent de-identified value within the same project. This enables disparate de-identified datasets to be safely linked together.				
Clients can choose to deploy the de-identification mechanism within their own system boundary and maintain their own private identifier mapping database. They can also choose to have a "Trusted Third Party" perform this operation using Aridhia software, but Aridhia will have no sight of the mapping information.				

When designing the de-identification service we have taken into account the legislation, international standards and best practice our client may need to comply with such as the Data protection Act 1998, the NHS England IG Toolkit, the Caldicott Principles and the and the European Data Protection Directive 95/46/EC. Further detail is available on our **De-identification Datasheet**.