PP12

Good Transparency Practice: A Working Group Update

Authors: Lauren Hepburn, Abby McDonell*, Devaki Thavarajah*, Mahesh Swaminathan, et al.*
**lihepburn@outlook.com, amcdonell@privacy-analytics.com, devaki.thavarajah@phuse.global*

Current trends emphasise the importance of public disclosure and sharing of clinical trial documents and data. Sponsors may be required to make anonymised clinical documents publicly available to comply with health authority transparency regulations, or may choose to participate in voluntary data sharing to facilitate secondary research. This poster is designed by the Good Transparency Practice (GTP) project group (part of the PHUSE Data Transparency Working Group) to highlight guidelines and best practices that may be used to govern the anonymisation of clinical trial data for external sharing or disclosure. By outlining the distinct roles of the Data Controller, Data Anonymiser, and Data Recipient, the project aims to provide a means to achieve accountability and traceability through the anonymisation process, while providing assurance that privacy requirements are upheld.

Principles of GTP

1. Clinical trial data sharing should be conducted in accordance with the applicable regulatory requirement(s) and local legislature.
2. Anonymisation should adequately protect the privacy of patients and prevent a serious possibility of identifying individuals in the data.
3. Prioritise retaining the maximum amount of analytically-valuable information during the anonymisation process while maintaining patient privacy.
4. The chosen anonymisation strategy should be documented in an anonymisation report made available to the Data Recipient.

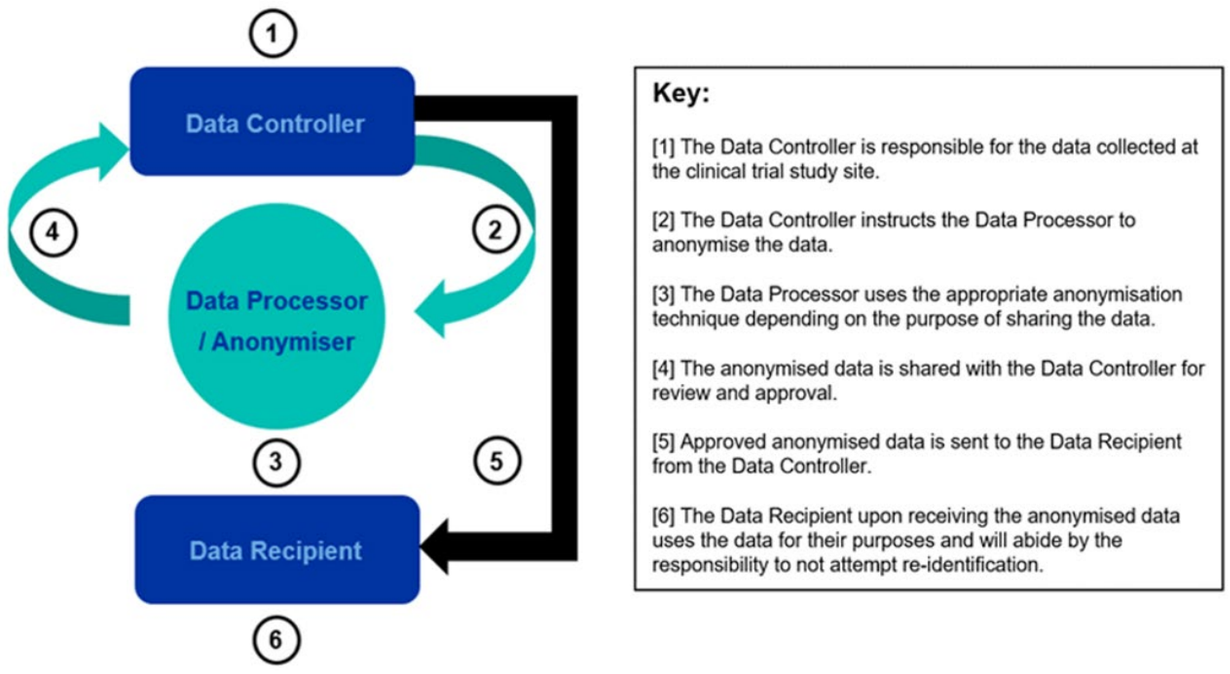

Figure 1: *Relationship between the Data Controller, Data Processor/Anonymiser, and Data Recipient under GTP. The Data Controller is ultimately responsible for the data collected and should ensure quality assurance is maintained with the use of SOPs, record keeping, and Data Protection agreements if data processing is outsourced by a Data Processor/Anonymiser.*

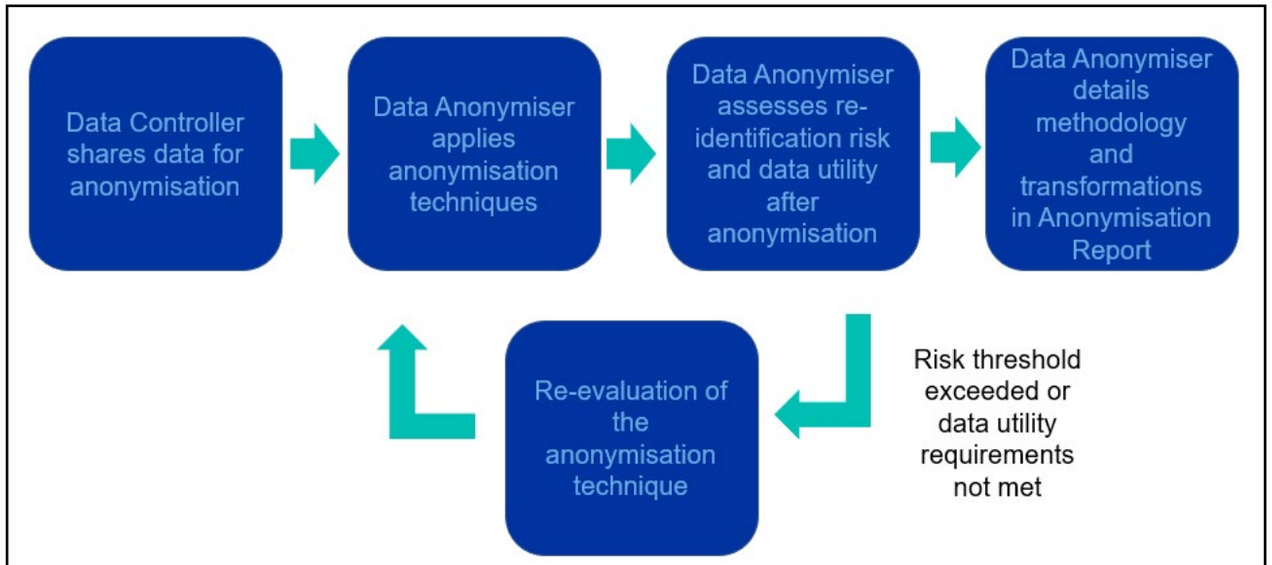

Figure 2: *Application of anonymisation strategy following the assessment of re-identification risk. The anonymisation strategy is selected by the Data Controller and applied by the Data Anonymiser. Both quantitative and qualitative risk assessments strategies may be used but should demonstrate how the chosen methodology results in a low risk of re-identification.*

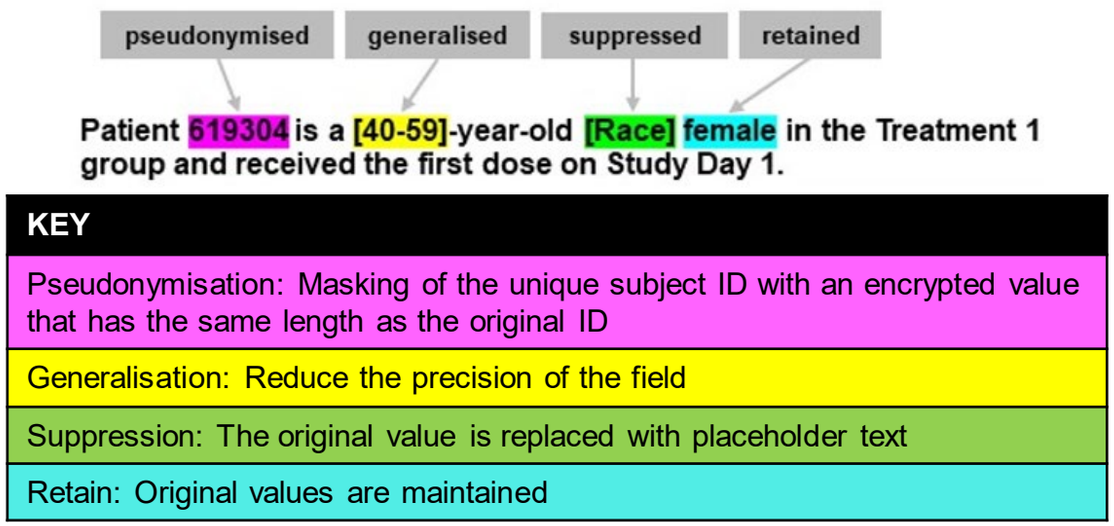

Figure 3: *Sample anonymisation strategy that is applied by the Data Anonymiser, approved by the Data Controller, and received by the Data Recipient. Multiple anonymisation strategies can be used to achieve low risk of re-identification and should be detailed in the anonymisation report.*