Queen Mary
University of London
Barts and The London

CANCER RESEARCH UK | BARTS CENTRE

Policy

Policy Title	De-Identification Policy
Policy Reference	BCC-ISM-Policy-03
Version Number	1.0
Approval Date	03/07/2019
Effective Date	24/07/2019
Review by Date	03/07/2020

Author:	Madalyn Hardaker Name	Information Governance Lead Position
Reviewed by:	Ivana Sestak Deeksha Prabhu Kristel Caisip Rachel Barrow-McGee Name	Lecturer in Medical Statistics Senior Research Applications Programmer Applications Developer Tissue Acquisition Officer Position

Approved by	Jonathan Croft Name	Head of Research Computing Position
	Signature	Date 03/07/2019

Version	**Release Date**	**Reason for Change**	**Updated By**
1.0	03/07/2019	N/A – First Release	Madalyn Hardaker

1. Policy Statement

1.1 Data Minimisation

In line with the General Data Protection Regulation (GDPR), only the minimum amount of personal data necessary for the purpose should be used. Staff should therefore only have access to the data that is necessary for the completion of the research or business activity which they are involved in; therefore, it may be appropriate in some instances for staff working with the same datasets to have different views or access levels. Similarly, it may be appropriate to store de-identified versions of datasets for extended periods of time even after the personal content of the dataset is due for destruction.

1.2 Limitations of de-identification

De-identifying data reduces the risk of personal data breaches and facilitates further application of valuable data assets for research that may otherwise be difficult or impossible due to legal or ethical concerns for privacy and confidentiality. At the same time, however, de-identification may also limit the data to such an extent that it no longer has sufficient value for the intended research purpose. Appropriate methods and statistical techniques must be used to ensure the data retains as much utility as possible.

1.3 Context Control and Safeguarding

De-identification is heavily context-dependent, so both direct and indirect identifiers must be considered within the processing environment, including other data and resources available, in order to determine the appropriate level of safeguards required. Technical and organisational safeguarding measures must be applied when there is any reasonable possibility that a data subject could be re-identified. In most cases of research projects involving human subjects, the ethics and regulatory review and approval processes will be one such means of ensuring adequate safeguarding.

1.4 Anonymisation

When data is truly anonymous, such as summary statistics and trend analyses, additional safeguards are not required because the data cannot in any way be linked back to an individual and is therefore not personal data and not subject to the data protection regulations.

There may be scenarios where pseudonymised data is shared within the confines of a legally binding agreement and is rendered "anonymised-in-context" for the recipient. In these scenarios the data is de-identified to the extent possible and then shared only within the terms of a legally binding agreement confirming further safeguards and that no attempts will be made by the receiving party to re-identify the data. The information which links the data back to the individuals it pertains to may still be held at the originating institution, and there may still exist extraordinary circumstances in which the dataset could potentially be re-identified, but the contractual agreement holds the receiving institution accountable for maintaining anonymity. These agreements must be reviewed and approved by an authorised signatory from each institution.

2. Additional Resources

Forms and Templates

n/a

Policies and Procedures

BCC-ISM-WI-01 Techniques for Dataset De-Identification

BCC-ISM-SOP-02 De-Identification

BCC-ISM-SOP-03 Data Sharing

BCC-ISM-Policy-04 Data Sharing

Regulatory Guidance

EU General Data Protection Regulation (2016)

UK Data Protection Act (2018)

Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques
https://www.pdpjournals.com/docs/88197.pdf

Other

Anonymisation: managing data protection risk code of practice (Information Commissioner's Office) https://ico.org.uk/media/1061/anonymisation-code.pdf

The anonymization decision-making framework (University of Manchester, University of Southampton, the Open Data Institute, and the Office for National Statistics) http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf

Understanding Patient Data (Wellcome Trust, Medical Research Council, Department of Health and Social Care, Public Health England, Economic & Social Research Council) https://understandingpatientdata.org.uk