BHBIA Data Analytics Guidelines
Secondary Data – Ethical Principles

These guidelines are part of a series designed to provide guidance on the legal and ethical issues impacting data analysts

INTRODUCTION

The growth in new technologies and our increased ability to process data more easily, more quickly and in larger volumes raises ethical issues around data sharing, compiling, storing, confidentiality, privacy and security. It is essential that secondary data is protected and processed in an ethical manner and in compliance with all the laws and regulations that apply to the data. **Just because you have access to the data does not mean that you can ethically or legally re-use the data for your intended analysis, purpose or research.**

SECONDARY DATA CONTAINING PERSONAL OR SENSITIVE PERSONAL DATA

Ethical concerns about secondary use of data most frequently revolve around potential harm to individual data subjects and will depend upon the nature of the data. Re-use of any data containing personal or special category (sensitive) personal data needs to be very carefully considered.

If the data has no identifying data (anonymised) or has been appropriately de-identified (pseudo-anonymised) and the data user cannot reverse the de-identification, then the risk of harm is greatly reduced although not completely removed. However if the data contains personal data the data controller and processor must be able to explain why it needs to be used, have the appropriate consents and ensure that appropriate privacy and data protection steps have been taken. The use of personal data must always comply with Data Protection law.

OPEN ACCESS SECONDARY DATA

Secondary data that is freely available on the internet, via publications or public forums is often assumed to be free from restrictions on use however permission for further use may be subject to restrictions.

Data of this type is often covered by an 'open data licence'. You should always check what the data can be used for and permission should be gained from the data owner for any re-use not covered by a license. In all cases the original source should be referenced and in most cases a hyperlink should be provided to the original online source.

PURCHASED SECONDARY DATA

Purchased data must only be used under the terms and conditions of the license or contract from the data supplier or source. It is essential that contracts are respected and that data is not used, processed, shared, or distributed beyond the limits contractually agreed or covered by the license. Data stored and supplied in a database may also be protected under UK Copyright and Database regulations.

Before sharing any purchased data you must have the permission of the data provider; they may require Third Party Agreements (TPA) between the supplier and the third party. Vendors often protect their data through seeding or similar methodologies so you can be caught out if you mis-use it (deliberately or accidentally). An example of this could be using a mailing list more than the licensed number of times.

CUSTOMER SOURCED SECONDARY DATA

Secondary data and analysis may be sold or shared directly or indirectly between a pharmaceutical company and their customers (e.g. healthcare providers and commissioners, pharmacy groups). In this situation companies must ensure that secondary data purchased or exchanged should not appear or be intended to influence or reward a decision to recommend the company's products or services.

SECONDARY DATA SECURITY

Market researchers and data analysts have a responsibility to their employers', the data owners and data subjects to ensure that their data is secure and protected from loss, theft, corruption and misuse.

Organisations of all sizes must have appropriate organisational and technical measures (e.g. adequate Data Security Plans) in place to protect secondary data, these may include:

- Commercially valuable or personal data should only be shared if encrypted e.g. by secure FTP transfers.
- Hardware such as laptops and tablets should have appropriate password protection.
- Personal data should not be transferred on un-encrypted emails, data sticks etc.
- Data that is no longer needed should be deleted or archived securely.
- Software security should be regularly maintained and updated.

Failure to take adequate steps to protect data, especially personal and sensitive personal data can result in disruption of service, loss of commercially valuable data and could have legal implications.

Some client companies audit and inspect suppliers that process data on their behalf for appropriate data security standards, third party vendors can be seen as a weak link in the data security chain.

REPORTING, PUBLISHING & REFERENCING SECONDARY DATA ANALYSIS

When reporting secondary data your analyses, interpretation and conclusions must reflect the data appropriately and accurately. Reporting must distinguish between factual reporting of data and interpretation.

Reporting must also include the technical detail necessary to assess the validity of the findings, such as data size, type, data collection method, statistical tests used.

The reporting or publishing must clearly reference the sources. Licenses or the terms and conditions often require this.

DO

- ✓ Check that you have permission to use the data for your intended purpose under the terms and conditions of the contract or license. If in doubt contact the data owner for permission.
- ✓ Keep all secondary data secure; protect it from theft, unintentional use, destruction or damage.
- ✓ Maintain the anonymity, confidentiality and privacy of data subjects by anonymising or pseudo-anonymising the data before secondary use. Only re-use personal data if it's absolutely necessary, with the informed consent of the data subject and in accordance with Data Protection law.
- ✓ Avoid harming any data subjects through the re-use of their personal data.
- ✓ Share secondary data only on a need to know basis.
- ✓ Follow all the appropriate data security processes to protect the data.
- ✓ Reference secondary data appropriately in reports and publications.
- ✓ Keep the secondary data accurate.

DON'T

- × Use or re-use secondary data in any way that would bring you or the pharmaceutical industry into disrepute, reduce confidence or breach laws and regulations.
- × Re-use, share or distribute secondary data, especially personal data and sensitive personal data unless you are legally and contractually allowed to do so.
- × Transfer secondary data via insecure channels.
- × Re-use personal data unless it is absolutely necessary and then only in accordance with Data Protection legislation.
- × Move data around between territories e.g. transfer it from Switzerland to India.

For further information see:

The Information Commissioners Office website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

CASRO Information Security: ISO 27001 Certification: https://www.iso.org/isoiec-27001-information-security.html

The National Archives – Information Management Licensing: http://www.nationalarchives.gov.uk/information-management/re-using-public-sector-information/licensing-for-re-use/

Copyright and Database Rights: https://www.gov.uk/copyright

This guidance is provided by the BHBIA for information purposes only and is not intended and should not be construed as regulatory or legal advice. It does not cover all legislative and regulatory requirements pertaining to Members and it is the responsibility of all Members to familiarise themselves with these.

The Guidelines are provided by the Data Analytics Guidelines Team within the BHBIA's Ethics & Compliance Committee,

Jason Bryant, Data Analytics Team Lead
Darren Kottler, Data Analytics Team
Klaas Breukel, Data Analytics Team
Catherine Ayland, BHBIA Ethics Advisor

If you have any queries about these Guidelines, please visit www.bhbia.org.uk and submit your query via 'My BHBIA' dashboard. Please note: this ad hoc advisory service is available to full BHBIA members only.

British Healthcare Business Intelligence Association
Ground Floor, 4 Victoria Square, St. Albans, Herts AL1 3TF
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk

A Private Limited Company Registered in England and Wales No: 9244455