BHBIA

bhbia.

Your essential guide

Legal and Ethical Guidelines for Healthcare Data Analytics

August 2025

Welcome to your guide to the legal and ethical requirements of carrying out data analytics work in the UK healthcare market.

We've been supporting the UK market research community since 2005 with our Legal and Ethical Guidelines for Healthcare Market Research – to help us all reduce risk, improve performance and make life a little simpler by drawing key information together in one place.

We are delighted to now be able to support data analytics in the same way. We previously offered a series of short guides for analysts and these have now been consolidated into this comprehensive document.

Of course, we review our guidelines regularly, keeping them up to date with the impact of any relevant legislation or other industry guidelines.

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

We hope you'll find the guidelines helpful and easy to use.

The Guidelines are maintained by the BHBIA's Ethics & Compliance Committee, within which the Data Analytics Guidelines team is dedicated to providing clear guidance to all those involved in healthcare data analytics.

BHBIA Ethics & Compliance Committee (View Committee members here)

British Healthcare Business Intelligence Association

If you have any queries about these Guidelines, or any legal or ethical questions about UK healthcare data analytics that aren't answered here, please visit www.bhbia.org.uk and submit your query via Guidelines > Request Advice.
(Note: this ad hoc advisory service is available to full BHBIA members only).

CONTENTS

UPDATED LEGAL & ETHICAL GUIDELINES – CHANGES AT A GLANCE

Changes have been made in the following areas and are highlighted by arrows throughout the Guidelines.

Revised Guidance Page 6

Section A – You

Additional roles have been added:

- Business / Data Analysts
- Sales Force Sizing / Market Opportunity Sizing (market modelling, advanced analytics, predictive analysis)

Revised Guidance Page 9

Section C – Ethical Principles for Handling Data – Key Considerations

An additional point has been added to section 3, Data Security:

- If data is being stored on a cloud based system or via a 2-way data passage with a third party data provider, make yourself aware of the data protection they offer, and that this is fit for purpose.

Revised Guidance Page 12

Section D – Data Protection – Rights of data subjects – Data Protection

Under section 4.1, Data Protection the following has been revised:

Existence of any automated decision making and its consequences. When profiling a subject they are entitled to understand how the profile was created and what information underpinned the profile. They are entitled to change any aspect of the profiling information. You and your organisation remain responsible in understanding the profiling process and information used – be it AI generated or not, and that profiling information is used reasonably and ethically.

Revised Guidance Page 26

Section I – Managing Databases and CRM – Appropriate data and use – Personal Data

Under section 2.1, personal data, additional clarification had been included in the following point:

The company must make sure that any personal data on HCPs or other customers held within the CRM is up-to date and accurate, be this an in-house generated list or one purchased from a specialist list provider

Revised Guidance Page 31

Section K – Artificial Intelligence and Data Protection – Introduction and Key Principles

Definition of What is Artificial Intelligence (AI) has been updated.

AI Legislation and Regulatory Advice section has been updated.

AI and Consent section has been updated.

Ethics Principles covering AI has been updated.

Assessing AI tools has been included.

Privacy by Design has been removed.

Deleted Guidance

Section K – Artificial Intelligence and Data Protection – 4. Consents, requests, decisions and documentation

Section above including section 4.1 – Key questions to ask yourself when starting an AI project has been incorporated into the new sections above.

A WHO'S THIS FOR?

You

- If you're involved in any pharmaceutical or healthcare data analytics work within the business intelligence / customer insight arena, carried out in the United Kingdom, including the Isle of Man and the Channel Islands.
- If you're working in or for a BHBIA member company

Those responsible for the following roles could include, but are not limited to:

- SFE Analysts (sales ops, territories, incentive schemes, targets and forecasts etc.);
- Customer Analysts (HCP segmentation, CRM, quant research support, database admin);
- Insights Analysts (RWE support, CCG segmentation, HES, promotional response analysis, machine learning and artificial intelligence);
- Business / Data Analysts
- Sales Force Sizing / Market Opportunity Sizing (market modelling, advanced analytics, predictive analysis)

Revised Guidance
Page 5

These guidelines are based on the principles of good data management, ethical analytics practice and data protection law. They will help to support and protect you and the people you work with.

And remember, if you work in a:

- BHBIA member company, you must follow these guidelines. It's an important condition of your membership. The same goes for the **BHBIA Legal and Ethical Guidelines for Healthcare Market Research** and the **ABPI/BHBIA Guidance notes on collecting adverse events, product complaints and special reporting situations during market research** if conducting market research.

  When we refer to 'you' within the Guidelines, we mean BHBIA members.

- ABPI member company or their affiliate, you must also adhere to the ABPI Code of Practice and you are accountable for the market research activities of your third party suppliers. Whilst the BHBIA's guidelines take into account ABPI requirements that affect data analytics, additional training on the ABPI Code for third party suppliers may be required by the end client/ABPI member company.

And your connections

If you work in a BHBIA member company, you must make sure that all relevant colleagues, clients, contractors and subcontractors are familiar enough with these guidelines to be able to satisfy them, and that their working arrangements comply fully with them.

We recommend that you include a clause in contracts and Master Service Agreements that commits everyone involved in a data analytics project (i.e. the commissioning company, any external agencies and any subcontractors) to following these guidelines.

B HOW WILL IT HELP?

You have the key information you need in one place to make sure your data analytics project goes smoothly from a legal and ethical point of view. By using this guide, you can minimise the chance of things going wrong, which wastes time and could even lead to prosecution. And you can gain in positive ways too.

✘

- Avoid breaking the law
- Avoid ethical errors
- Avoid damaging your professional or company reputation

✓

- Find information quickly, saving time and money
- Impress colleagues with your knowledge and expertise
- Create consistency across your projects

We make a distinction between actions that we advise you to take and those that are compulsory. When we're advising, we say *should*. When it's compulsory, we say *must*.

Whilst some of this document covers best practice advice, much of the content relates to data protection and other legislation, so aside from your BHBIA member obligations, it is a legal requirement that you follow it.

We also recommend that you familiarise yourself with the key words and phrases set out the Appendix – in particular the Data Protection Legislation and Key Terminology sections. This Guide is based on the legislation and codes listed under Sources, and we recommend that you familiarise yourself with these.

C ETHICAL PRINCIPLES FOR HANDLING DATA – KEY CONSIDERATIONS

1 Introduction

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.

Data must:

- Be protected
- Be processed in line with ethical and legal requirements
- Not be used or interpreted / presented in such a way that would bring you or the pharmaceutical industry into disrepute.

Just because you have access to the data does not mean that you can ethically or legally use the data for your intended analysis, purpose or research.

2 Nature and source of data

2.1 Personal Data

Consider whether the data contains Personal or Special Category (Sensitive) Personal Data.
Ethical concerns about use of data most frequently revolve around potential harm to individual data subjects.

- Use personal or special category (sensitive) personal data very carefully.
- If the data contains personal data then Data Protection law applies.
- Consider the source of the data

2.2 Open Access Data

- You and your organisation should consider how the data has been collected. Some tools may use unethical practices for collecting data, even if their license allows you to use it freely
- Data that is freely available on the internet, but may be subject to restrictions.
- Data of this type is often covered by an ‘open data licence’.
- Always check what the data can be used for and gain permission from the data owner for any re-use not covered by a licence.
- In all cases the original source should be referenced and in most cases a hyperlink should be provided to the original online source.

2.3 Purchased Data

- Only use purchased data in line with the terms and conditions of the licence or contract.
- 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.

2.4 Customer Sourced Secondary Data

- Secondary data and analysis is sometimes sold or shared 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, eg if purchased data is shared then then the use of this data must be fair, balanced and non-promotional.

3 Data security

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.

- You should ensure you have appropriate organisational and technical measures (e.g. adequate Data Security Plans) in place to protect data.
- Failure to take adequate steps to protect data, especially personal and special category personal data can result in disruption of service, loss of commercially valuable data and could have legal implications.
- Some client companies audit suppliers that process data on their behalf for appropriate data security standards; It is important to ensure third party processors can provide evidence of competence regarding data security.
- The use of technology in the workplace to facilitate remote working has surged in recent years, and so has its use as it relates to business intelligence. A heightened sensitivity to online security is one of our new 'norms'.
- If data is being stored on a cloud based system or via a 2-way data passage with a third party data provider, make yourself aware of the data protection they offer, and that this is fit for purpose.

Revised Guidance
Page 5

The BHBIA has produced two guides, which you will find in the **Privacy & Data Protection** section of the website:

Online Security - Compliance: The New Normal

- Practical tips and suggestions to enhance online security.

Due Diligence and New Technologies - Compliance: The New Normal

- Helpful questions members can ask themselves when assessing new technology and doing their due diligence before using it on live projects.

4 Reporting, publishing and referencing

When reporting, your data analyses, interpretation and conclusions must reflect the data appropriately and accurately

- Distinguish between factual reporting of data and interpretation.
- Include the technical detail necessary to assess the validity of the findings, e.g. data size, type, data collection method, statistical tests used.
- In addition, you must make available if requested, details of any instruments used, any data cleaning, weighting or adjustments applied, and any substantive limitations affecting the validity of the findings.
- Clearly reference the sources. Licences or the terms and conditions often require this.
- Include the Date of Preparation and, if possible, the Refresh Date for the data.

D DATA PROTECTION

1 Data protection law

The GDPR (General Data Protection Regulation) and the UK Data Protection Act (DPA) 2018 control how personal data is used by organisations, businesses or government.

They regulate the processing of personal data across the European Union and the UK respectively, protecting the rights of individuals whom the data is about (data subjects), mainly by placing duties on those who decide how and why such data is processed (data controllers) and those that process the data (data processors).

Data protection law applies to anyone who is processing personal data.

The UK DPA 2018 enacts the GDPR into UK law. In June 2021, the UK's data protection regime was formally deemed 'adequate' by the European Commission. An adequacy decision allows organisations that transfer personal data from the EU (and the European Economic Area) to the UK, to continue to do so without restriction or additional safeguards.

For the latest information on data protection legislation, check the BHBIA's **Privacy & Data Protection** resource. These guides are particularly pertinent to data analytics:

- International data transfer mechanisms under the UK GDPR
- Data Security including Breaches and International Transfers
- Online Security - Compliance: The New Normal
- Due Diligence and New Technologies - Compliance: The New Normal
- Sharing Personal Data – Quick Guide
- Risk and Privacy Impact Assessment
- Legal Grounds for Data Processing

2 Processing Personal Data - definitions

Personal data is:

Any data relating to an identifiable living person which alone or in combination with other accessible information can identify the individual:

- E.g. a single piece or series of pieces of data which allow identification of a living individual
- Includes names, addresses, post codes, phone numbers, email addresses
- Alphabetical, numerical, graphical, photographical or acoustic
- Data kept on paper, stored in a computer memory or a video-recording

Personal data includes video-streams (relayed live or delayed and non-anonymised recordings) and may include audio recordings. Whether an audio recording is considered personal data depends on whether in the absence of any other identifiers the voice alone could lead to identification of the individual.

Special category (sensitive) personal data:

Refers to race/ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and offences (alleged or committed).

- Health data includes, but is not limited to genetic and biometric data.

Anonymising or pseudonymising the data before secondary use can help to maintain the anonymity, confidentiality and privacy of data subjects:

Anonymisation = removing, obscuring, aggregating or altering identifiers.

- Once all identifiers linking data to an individual have been removed in such a way that they can no longer be accessed then it is no longer personal data - it has been anonymised and is not covered by data protection law.

Pseudonymisation = personal data is removed and the 'record' is given a unique identifier.

- If personal data has been pseudonymised it will still be considered personal data if you retain the ability to re-identify the individual.

Processing personal data means:

- Obtaining, recording, storing data or carrying out any set of operations on the data. It is actually very difficult to think what an organisation might do with the data that would *not* be defined as processing.

Data Controller:

- A person who alone, jointly or in common with others, determines the data processing purpose and means (i.e.. both the client and the agency may be considered controllers)

Data Processor:

- An organisation or person (other than an employee of the same company) processing data in line with the instructions of the data controller. There may be more than one processor assigned to a project

See Section L Appendix - Data Protection Legislation for more information – including full definitions of personal data / special category personal data, the key principles of data processing and full definitions of data controller and data processor roles, plus a note about the data protection officer (DPO) role.

3 Lawful bases for data processing

Those processing personal data must have a 'lawful basis' for doing so and this must be documented.

The lawful bases that most commonly apply to data analytics projects are:

- **Consent** of the data subject*
- **Legitimate interest** (processing is necessary for the purposes of the legitimate interests of the data controller or a third party)
- **Contractual obligation** (processing is necessary for the performance of a contract)

> **Consent** *under GDPR/DPA 2018 refers to "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

Other bases exist, but these conditions are unlikely to apply to data analytics.

If the information is special category personal data - e.g. information about an individual's health, only explicit consent is likely to be relevant.

The term ***Privacy Notice*** refers to the oral or written statement that individuals are given when data about them is collected. The privacy notice must tell the individual - who you are, the purpose(s) for which you intend to process the information; and any extra information you need to give individuals in the circumstances to enable you to process the information fairly.

4 Rights of data subjects

4.1 Data Protection

The 'Data Subject' is the person to whom the particular personal data relates and the GDPR/DPA 2018 says that data subjects' have the following data protection rights:

- **The right to be informed**: This encompasses your obligation to provide 'fair processing information', through a specific agreement and/or privacy notice – for consent to be informed the agreement must include:

  - ✓ **Name of the organisation/individual** seeking consent and their **contact details**, if this is not the data controller you must identify the data controller
  - ✓ **Name any third parties who will rely on the consent i.e. any recipients of the personal data** (naming the type of organisation is not sufficient) e.g. the name of the commissioning client if they are to be given access to reports or results containing personal data
  - ✓ **Legal basis for processing** some business processes may rely on "legitimate interest" whereas others (like automated profiling) may require specific consent
  - ✓ **Purposes** of the processing – why you want the data
  - ✓ **Types of processing activity** – what you will do with the data
  - ✓ **Where processing is based** and **details of any data transfer to countries without adequate data protection** (generally countries outside the European Union - EU)
  - ✓ **How long the data will be stored** or if that's not possible, the criteria used to decide this
  - ✓ **Right to withdraw consent** at any point and other rights - to have their personal data rectified or erased, to access or move their data, to restrict or object to data processing in future and to complain to the data protection authority (the Information Commissioner's Office in the UK) - some of this detail could be put into the privacy notice. It must be as easy to withdraw consent as it was to give it, so it should be an easily accessible single step. It is good practice to tell individuals how to withdraw (including on the privacy notice).
  - ✓ **Existence of any automated decision making** and its consequences. When profiling a subject they are entitled to understand how the profile was created and what information underpinned the profile. They are entitled to change any aspect of the profiling information. You and your organisation remain responsible in understanding the profiling process and information used – be it AI generated or not, and that profiling information is used reasonably and ethically.
  - ✓ **Contact details of data protection officer**

Revised Guidance
Page 5

- **The right of access:** So that individuals are aware of and can verify the lawfulness of the processing
- **The right to rectification:** To have personal data rectified if it is inaccurate or incomplete (within 1 month)
- **The right to erasure:** Individuals have a right to have personal data erased in specific circumstances. This does *not* provide an absolute 'right to be forgotten' - if an individual has asked not to be contacted you must keep or have access to a 'do not contact' list or database to make sure you don't contact them
- **The right to restrict processing:** Individuals have a right to block processing of personal data. In this case you can retain just enough information to ensure that the restriction is respected in future
- **The right to data portability:** This allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way
- **The right to object:** Individuals have the right to object to (amongst other things) processing based on legitimate interests
- **Rights in relation to automated decision making and profiling (e.g. use of AI techniques):** Individuals have the right not to be subject to a decision when it is based on automated processing; and it produces a legal effect or a similarly significant effect on the individual

4.2 Privacy

Under the UK Data Protection Act 2018, and the European Convention on Human Rights states "*everyone has the right to respect for his private and family life, his home and his correspondence*."

In addition, individuals that are involved in market research (primary or secondary) as respondents or contributors (e.g. through passive digital listening) have the right to anonymity (their identity will not be revealed) and confidentiality (their identity will not be linked to their input), though they can choose to waive these rights.

If in doubt, be as specific as you can be on why you're handling the data.

For more information on the rights of data subjects, visit the **ICO website**.

5 Data Protection do’s and don’ts

If you process personal data make sure you understand what you can and can’t do with it!

Here we provide a set of basic do's and don'ts for handling personal data, based on the definitions, key principles and data subjects' rights covered in the previous section, which you can use as a checklist.

5.1 Things you must do

- **Make sure you understand what ‘personal data’ is and whether your data source includes it – and specifically whether it includes special category (sensitive) personal data**
  - If possible, anonymise or pseudonymise the data before secondary use to protect the data subjects.
- **Make sure you understand what data processing is and what your role is:**
  - Be aware of the 7 key data processing principles and the rights of data subjects.
  - Your role as controller or processor may change from project to project and can change within projects.
  - Data controllers must have written contracts with processors (e.g. sub-contractors) to ensure data security.
  - Make sure all those involved understand their responsibilities.
- **Have a specific and legal basis for the processing of personal data:**
  - Consent, legitimate interest and contractual obligation are most common, but only consent is likely to be relevant for special category data.
  - Process personal data only in ways that individuals would reasonably expect, and ensure that you avoid doing anything that could have adverse effects on them.
- **If you require consent to process personal data, this must be a clear affirmative action, freely given, specific and informed:**
  - Individuals must be made aware of who will have access to their personal data, for what purpose and any other information that would be required to ensure fair processing.
- **Only use personal data for the purposes for which it was collected:**
  - Only re-use personal data if it's essential
  - Any re-use of personal data must be compatible with the original purpose, so think ahead and ensure that any likely secondary uses of data are considered when gaining consents.
- **Make sure the personal data is secure and protected and that access is limited to those that ‘need to know’:**
  - Store personal data securely, with appropriate technological and organisational measures to safeguard the data
  - Ensure that only authorised people can access, alter, disclose or destroy the data.
  - Ensure that if the data is lost, altered or destroyed it can be recovered without harm to the individual.
- **Make sure you understand the terms and conditions attached to any personal data you want to process:**
  - Just because you can access it, doesn’t make it legal to use it, for instance, many websites provide data for personal use only, or prohibit commercial use, the copyright or licence may prohibit use of certain types of use. If in doubt, ask.
  - If you would like to use the personal data from a third party for a purpose that's not stated in their T&Cs, contact the supplier and state your request.
- **Make sure that when personal data is transferred it is protected by law:**
  - Make sure the transfer is essential;
  - Know exactly which countries it’s going to, what this means in terms of restrictions and plan your approach;
  - Have contracts in place with all involved parties;
  - Export the data securely.
- **If you plan to incorporate data into systems/databases:**
  - Remember that, regardless of the ownership of a database, any personal data within it will be subject to data protection law.
  - Check where the data will be held - restrictions apply, and can prohibit storage outside the UK or European Economic Area.
  - Be aware that data about living individuals recorded in CRM (Customer Relationship Management) systems or KAM (Key Account Management) tools is also covered under data protection legislation - be especially careful about data to be collected in free text fields.
- **Your company should have a policy that deals with data protection**
  - e.g. amongst many other things, it should tell you what to do if you are asked for a copy of the personal data you hold about them by an individual or what to do if an individual request that the personal data you hold about them is deleted.
- **If you process personal data you must pay a fee to the Information Commissioner’s Office:**
  - This applies to every commercial organisation whether you are a large multi-national or a sole trader. Once registered you must keep your registration up to date - e.g. update it if you change any of the purposes for which you use data.

- **If you are using the personal data as part of a full automated decision-making process, which has a direct impact on the data subject, be aware of the requirements:**
    - This is also known as 'profiling'. There are more specific and stringent legal requirements - see more details on the ICO website here
- **Assess the level of risk in your data processing:**
    - Decide whether a Data Privacy Impact Assessment (DPIA) is needed

5.2 Things you must not do

- **Do not collect personal data or hold it in datasets unless you have to.**
- **Do not collect or hold personal data without a specific and legal reason to do so.**
- **Do not re-use personal data for a purpose that is incompatible with the original purpose.**
- **Do not hold or collect more personal data than is required or justified by the purpose.**
- **Do not store personal data for longer than it is needed.**
- **Do not keep inaccurate data or use out of date data where inaccuracies could occur - either update it or delete it:**
    - This can be particularly problematic where secondary data was purchased as a one-off in the past.
- **Do not provide personal data to others without:**
    - Ensuring that you are legally and contractually allowed to do so.
    - Informing them of the appropriate purposes for which it can be used.
    - Ensuring the security of the data at all times.
- **Do not export or transfer personal data overseas, or move data around between territories, unless it's essential**
- **Do not transfer data via insecure channels e.g. to/from personal email accounts**

6 Risk and Privacy Impact Assessments

6.1 Assessing risk

All those processing personal data for commercial purposes are required to demonstrate that they comply with the data protection law - this requirement is referred to as 'accountability'

- As the GDPR/DPA 2018 distinguish between higher and lower risk data processing activities and the requirements for these two differ, it is essential that all those processing data can assess the level of risk associated with their activities.
- Data protection law demands that organisations take a "*risk based approach*" to data protection. So you need to understand when and how to go about assessing risk.

Although 'risk' is regularly referred to within the GDPR/DPA 2018, it is not defined. It is generally associated with the risk of inappropriate access and disclosure. Assessing risk means you have to think carefully about the "likelihood and severity" of any negative impact on individuals.

The ICO recommends that to examine data processing activities in terms of risk assessment you should take a three-pronged approach, this may be termed a **preliminary risk assessment:**

1. **Identify any potential threats that could do harm** - e.g. excessive collection of data, inadequate records, inappropriate access, misuse, loss of data, excessive sharing, over-retention
2. **Evaluate the severity of the harm** - this is likely to involve evaluating how sensitive, valuable and critical the data are
3. **Consider the likelihood of the harm occurring**

2 and 3 will require you to think about (amongst other things): Where will the data be stored?, How secure is that?, Who has control?, Will it be transferred?, Who would be responsible for data loss?

The next step is to apply cost-effective actions to mitigate or reduce the risk.

6.2 When to conduct a DPIA

Data protection impact assessments (DPIA, also known as privacy impact assessments or PIAs) are the practical tool required by the GDPR/DPA 2018 to assist organisations in the risk assessment process. They help you with identifying, assessing and reducing the data protection risks of your project and identifying and evaluating privacy solutions.

A single DPIA can be carried out covering a set of similar processing operations that present similar high risks e.g. for very similar data analysis projects.

DPIAs SHOULD be carried out when:

- The data processing might result in a high risk to the rights and freedoms of the individuals
- If you are not sure whether your data processing is high or low risk, you need to carry out a DPIA – if in doubt, carry one out!

DPIAs MUST be carried out when:

- Large scale processing of personal data that affects a large number of individuals; and involves a high risk to their rights and freedoms
- Large scale processing of special category personal data
- Using new technologies and the processing is likely to result in a high risk to rights and freedoms
    - Automated processing, including profiling, that results in automated decisions having legal effects or similar significant impacts on the data subjects - Profiling is any form of automated processing intended to evaluate certain personal aspects of an individual (e.g. personalised targeted direct mailings); profiling is not the same as market research segmentation.
- Systematic monitoring of a publicly accessible area on a large scale.

What does 'large scale' mean?

The GDPR/DPA 2018 does not define ‘large scale’. The European Data Protection Board (EDPB) recommends that the following factors are considered when determining whether processing is large scale:

- The number of data subjects concerned - either as a number or as a proportion
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

The EDPB also provides some examples of large-scale processing which include the processing of patient data in the regular course of business by a hospital. An example that would not be considered large-scale is the processing of patient data by an individual physician.

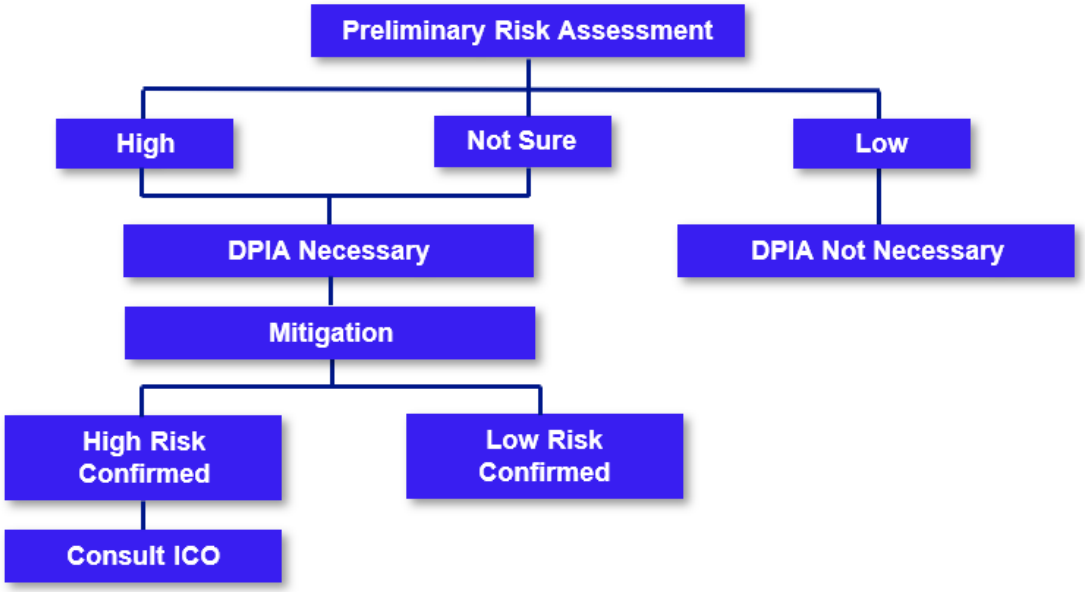
Organisations should ask themselves:

- Do we carry out potentially high-risk data processing?
- If the personal data was disclosed how likely is it that this would have a negative impact and how severe would this be?

6.3 The DPIA process

The ICO advise that a DPIA should contain:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller, or the consent provided by the data subject
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An assessment of the risks to individuals
- The measures in place to address risk, including security and to demonstrate that you comply e.g. quarantining data, deletion, redaction, encryption; restricting and controlling access and the technical and organisational measure taken to do these things.



Overview of the DPIA Process

Once the DPIA has been conducted you can sign off and record the DPIA outcomes and integrate the outcomes into any project plan.

- When a DPIA indicates high risk data processing even after mitigation you will have to consult the ICO to seek its opinion as to whether the processing operation complies with data protection law.

For further information on how to conduct a DPIA see the ICO's guidance and template

E PURCHASING, USING AND SHARING DATA

1 Sharing data

Analysts must verify the provenance of any personal data that is shared with them for processing. To do this it is likely to be necessary to request information from the data supplier or commissioning company. It is your responsibility to satisfy yourself about the integrity of the data supplied to you. You should make appropriate enquiries and checks e.g. about the data source or usage rights, including the following:

- confirm the source of the data;
- identify the lawful basis on which it was obtained and that any conditions attached;
- check what individuals were told at the time of handing over their data;
- verify details of how and when the data was initially collected;
- check the records of consent, if you are relying on consent;
- review a copy of the privacy information given at the time of collection of the data;
- check what information was given to individuals i.e. privacy information;
- check that the data is accurate and up to date;
- and ensure that the data you receive is not excessive or irrelevant for your needs.

2 Sharing data which your company has purchased

Data you have 'purchased' from a data vendor as part of a syndicated service is likely to be licensed to you, i.e. you have the right to use the data but you do not own it.

Notes:

- *In this section we are referring to the sharing of aggregated (non-personal) information such as sales, activity, segmentation etc. and looking purely at the considerations in relation to your agreements with the vendor. The guidance here does not cover the scope of "personal data" such as Health Care Professional (HCP) records or sub-sets / segments of these, which is covered elsewhere in this guideline.*
- *Open Access Data - e.g. HES Data from NHS England is covered later - see Section G*

If you need to share the data externally with a third party e.g. an analytics provider, consultant or an agency, you should check the re-distribution rules within the terms of the agreement/contract.

- The re-distribution rules will dictate if and how you are allowed to share the licensed data. Often you'll be expected to complete a request for a Third Party Agreement (TPA) before any data can be shared with a third party. A TPA is an agreement which is signed by the 3 parties – the data vendor, the third party and yourself. TPAs are used to protect the data vendor from mis-use of their data
- Bear in mind also that data is often protected (or "seeded") by the vendor so any onward usage is likely to be detected.
- If you are in any doubt at all check with all vendors involved; supplier of the data, recipient(s) and any intermediaries e.g. analytics providers.

3 Presenting 'purchased data' outside of the company

If you want to present licensed data externally to non-company employees e.g. at a conference or as part of a detail aid, then you should obtain permission from the data vendor to do this.

The data vendor will generally want to:

- know when and how it will be presented, and to whom
- see the data as it will be presented along with any additional data sources, commentary or text
- check that any statements and assumptions you make about the data are fair and accurate and will also confirm how the data should be sourced.

4 Ownership of data analytic tools intellectual property

When a data analytics tool is purchased, generally the purchaser/user won't own the rights to the Intellectual Property (IP).

- IP rights for data analytic tools are generally owned by whoever built the tool but the IP rights may have been passed to the purchaser. This should be checked within the contract.
- Without the IP rights a tool cannot be reproduced e.g. if a forecast model was built, the purchaser couldn't re-create it themselves and re-use if they didn't own the IP.
- You may be able to use screenshots showing the tool but you are advised to obtain written permission from the vendor as the design of the screens or models are likely to be their IP.

5 Referencing of data

Reference your data correctly whether it's within a spreadsheet, report or presentation. This ensures the recipient has a clear understanding of how the data were derived and makes it easier should the dataset need to be updated.

Specifics to include:

- Name of data source - Market definition (inclusions and exclusions)
- Detail of data measure (if this is not clear within data presented) and currency
- Country/region definition if applicable e.g. Europe = x countries or UK = retail pharmacy data only
- Snapshot / time of data extract to illustrate currency

F EXPORTING PERSONAL DATA OUTSIDE OF THE UK

Data protection law imposes restrictions on the transfer of personal data outside the UK and the European Union (EU) to make sure that protection travels with the data.

Many organisations involved in business intelligence need to transfer personal data from one country to another.

However, it is always worth asking whether the purpose can be achieved without the use of personal data – i.e. Can the data be anonymised so that data protection requirements don't apply?

You will find it useful to refer to the following guide in the **Privacy & Data Protection** section of the BHBIA website, in particular *the International data transfer mechanisms under the UK GDPR* guide.

1 Transfers and restrictions

International transfers of personal data for processing may be made from the UK to:

1. Countries within the EEA, with no restrictions
2. Non-EEA countries where the European Commission (EC) decided before 31 December 2020 that an adequate level of data protection is provided; this 'adequacy decision' establishes that a non-EU country provides a level of data protection that is essentially equivalent to that in the EU (this now includes the UK). Non-EEA countries are covered by adequacy regulations issued by the UK ICO
   The Information Commissioner's Office provides a list of countries providing adequate protection for UK data subjects in connection with the processing of their personal data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/
3. Organisations in countries not covered by 1 and 2 above where appropriate safeguards have been put in place e.g. standard contractual clauses.
4. Organisations in countries not covered by 1 and 2 above where exceptions can be made because specific conditions apply e.g. the transfer can be made as the data subject has given their informed consent

Servers or cloud systems used to store personal data need to reside in approved countries too, in order to avoid the need for additional arrangements.

If you are processing data in a non-EU country or a country without an adequacy decision, you will need to consider the following:

- Data subjects will need to be informed that their data is being processed in the relevant country
- Security arrangements for the transfer of data will need to be considered and documented (e.g. use of encryption technology).
- Privacy notices must include information about details of any transfer to a third country plus details of the safeguards and the means by which to obtain a copy of them or where they have been made available.
- An appropriate contractual arrangement needs to be in place with the company receiving the data.

2 Circumstances and safeguards for transfer

The following mechanisms exist to facilitate safe transfer of data outside of the UK/EU:

2.1 Transfers on the basis of a European Commission Adequacy Decision

- International transfers of personal data may be made where the EC decided before 31 December 2020 that a third country (a non-EU country), a territory or one or more specific sectors in the third country, or an international organisation ensures an 'adequate' level of protection.
- The UK's data protection regime has been formally deemed 'adequate' by the EU. An adequacy decision allows organisations that transfer personal data from the EU (and the European Economic Area) to the UK, to continue to do so; there is no need to put alternative transfer mechanisms (such as standard contractual clauses (SCCs)) to be put in place.
- All countries belonging to the European Economic Area – the EEA – are considered by the EC to have adequate data protection in place. See the European Commission website for a list of non-EEA countries also considered to have adequate data protection.

2.2 Transfers subject to appropriate safeguards

(for transfers to 'third countries' (countries without an adequacy arrangement in place – e.g. China.)

You may transfer personal data when the organisation receiving it is subject to appropriate safeguards and on condition that enforceable data subjects' rights and effective legal remedies are available. The appropriate safeguards include:

- Standard contractual clauses (SCCs): These enable the free flow of data when included in a contract or added as an appendix to a contract. They cover the contractual obligations between both parties to protect the rights of the individuals whose data is being transferred.

  Updated EU SCCs have been developed by the **European Data Protection Board (EDPB)** and are now available for transfers from the EU.

  However, the EU SCCs do not apply for transfers of personal data from the UK to a third country. New mechanisms for transfers from the UK were introduced in March 2022:

  - International Data Transfer Agreement (IDTA): this is a UK equivalent to the EU's standard contractual clauses (SCCs).
  - UK Addendum to the EU SCCs: this can be appended to EU SCCs reducing the need for organisations to use both EU SCCs and the UK IDTA.

  From September 2022, the old, legacy EU SCCs can no longer be used, and from March 2024 all contracts need to incorporate the new mechanisms.

  See the BHBIA's *Data Security, Breaches and International Transfers* guide in the **Privacy & Data Protection** section of the website for full details and the **ICO's international data transfer agreement and guidance** for full details

- Binding corporate rules (BCRs): Agreements governing transfers made between organisations within the same corporate group or a group of enterprises engaged in a joint economic activity but not necessarily forming part of the same corporate group

Under UK GDPR/DPA 2018 there is no longer a requirement to give prior notification to and seek authorisation from Data Protection Authorities when transferring personal data to a third country based on SCCs or BCRs.

2.3 Other transfer options - derogations

The UK GDPR/DPA 2018 provides derogations – exemptions – from the general prohibition on transfers of personal data outside the UK/ EU for certain specific situations:

- Made with the individual's informed consent after having been informed of the possible risks associated with such a transfer in the absence of an adequacy decision and appropriate safeguards
- Necessary for the performance of a contract: ─ between the individual and the organisation ─ made in the interests of the individual between the controller and another person;
- Necessary for important reasons of public interest
- The transfer is made from a register available to the public or any person with a legitimate interest
- Necessary for compelling legitimate interests of the Data Controller - in certain very specific circumstances - if no other transfer means is available and the transfer is one-off or infrequent and involves only the data of a limited number of individuals.

There are other derogations but these are unlikely to be relevant to commercial healthcare business intelligence.

Consent agreements and privacy policies must include details of any transfer outside the UK/EU.

The country should be named and if possible in the privacy policy a link to the adequacy mechanism used should be provided. In addition, details of safeguards (or at least a link to them) should also be provided.

Examples of data transfer scenarios

1. A UK based data collection and processing company has decided to out-source their UK personal data processing to a third party based in India (for marketing segmentation & targeting activities).

Prior to sending any personal data from the UK to India the UK company should determine if this activity cannot be achieved by using anonymised data. If not then the UK company must establish a contract with the Indian company that ensures adequate protection under the UK Data Protection Act. This may involve self-assessment; contractual clauses and Binding Corporate Rules approved by the Information Commissioner's Office or be covered by exceptions from the rules.

2. A global CRM company has sold its on-line software and applications platform to a UK pharmaceutical company. The CRM servers will be based in Belgium and personal data from the current UK based system will be transferred to the Belgium platform.

Belgium is a member state of the European Union and as such personal data can be transferred from the UK to Belgium without restrictions. The UK has designated EEA member countries as providing an adequate level of protection (of personal data for the purposes of the UK GDPR).

G OPEN ACCESS DATA

Open data is also referred to as Open Access or Public Access Data

It has gained in popularity, with developments such as 'data.gov.uk' – the open-data government initiative and the availability of the NHS England Hospital Episode Statistics, all which make data that is particularly relevant to the pharma/healthcare industry available under open licence.

Open data must have a licence that states that it is 'open data'; without a licence the data cannot be re-used in any way. The licence will state the uses that the data may be used for.

Open Data is protected

Whilst the open licence is designed to enable everyone to use the data for the benefit of the wider society, various laws and legislation still apply to open data:

- Copyright Laws
- Database Rights
- And where personal data is available Data Protection law (based upon the GDPR / DPA 2018) and the Freedom of Information Act 2000 apply.

1 The Open Government Data Licence

What does the Open Government Data Licence cover?

This licence is designed to enable anyone to use the data to the benefit of the wider society. Most open data sources have few restrictions, but some do not allow commercial use, so you should check carefully.

You are free to:

- Copy, publish, distribute and transmit the information.
- Adapt the information.
- Exploit the information commercially and non-commercially; for example, by combining it with other information, or by including it in your own product or application.

When you do any of the above you must:

Acknowledge the source of the information in your product or application by including or linking to any attribution statement specific to the Information Provider(s) and, where possible, provide a link to this licence.

But beware, the use of personal data has additional caveats!

The Open Government Licence does not cover the use of personal data. This is because any re-use of personal data must comply with data protection law (as covered elsewhere in this training).

2 HES data from NHS England

2.1 What is HES data?

Hospital Episodes Statistics (HES) is a data warehouse containing details of all admissions, outpatient appointments and A&E attendances at NHS hospitals in England.

This data is collected during a patient's time at hospital and is submitted to allow hospitals to be paid for the care they deliver. HES data is designed to enable use for non-clinical purposes, of this administrative data. This is known within the NHS as SUS (Secondary Uses Service).

The data are provided and licenced through NHS England (formerly the Health and Social Care Information Centre - HSCIC), the organisation responsible for the guardianship of NHS data in England.

- HES data can only be shared for "the purposes of the provision of health care or adult social care, or the promotion of health". It cannot be used for "solely commercial purposes" - e.g. targeting and segmentation or field force alignment.
- The basic principle is that patient data should ultimately only be used to benefit patients; each separate use of the data needs to be justified.

- You must also ensure that your use of the information does not breach the Privacy and Electronic Communications (EC Directive) Regulations 2003 or Data Protection law.

2.2 Using HES data

HES Data is available in a variety of ways, each of which have different implications.

Tabulated data:

NHS England can provide tables of aggregated data to answer specific questions. A wide variety of data is published on the internet, or requests for specific data can be made via enquiries@nhsdigital.nhs.uk. Any data provided will be published on the NHS England website or can be provided as a monthly extract if you complete the applications form and it is accepted.

Patient level data:

NHS England can provide patient level data for analysis.

- NHS England is careful to ensure that it understands the exact purpose for which the data will be used, and will look to provide the minimum level of data required to fulfil this purpose.
- Data is typically pseudonymised, meaning that identifying fields such as name, address and date of birth are removed (i.e. it is anonymised as far as the user is concerned).
- Higher levels of scrutiny are applied the more sensitive the data that is requested.
- Use of data is restricted to certain purpose(s), which will be identified in your Data Sharing Agreement.

Applications for data are scrutinised by a semi-independent committee (AGD) on behalf of NHS England, whose mandate is to ensure the acceptable use of data - see information on the application process and what is available on the NHS England website

Any organisation holding, or with access to patient level data (including pseudonymised data) may be asked to provide assurance on data security by completing the Data Security and Protection Toolkit (dsptoolkit.nhs.uk)

Data Intermediaries

Data can be provided by data intermediaries – companies that have applied for data and process it on behalf of others.

- Data intermediaries have permission to provide data to particular types of organisations for specific purposes and should make you aware of this
- NHS Digital publishes a list of current releases which set out the purposes for which each organisation can use the data.
- Typically data provided are aggregated and masked (small numbers hidden to prevent accidental identification of patients).

Justification of use

When obtaining patient level data from data intermediaries or reapplying for further data of your own, you often have to provide evidence of benefits to the health and social care system delivered from your use of the data to date. Increasing the knowledge within a particular area of medicine is not deemed to be a benefit in itself. NHS Digital then use this to justify the ongoing provision of data.

When applying for patient level data, NHS England will need to be assured that:

- the data will only be used for the purposes for which it was applied
- that these purposes have a clear mechanism for delivering patient benefit
- that these benefits can be evidenced in the future
- that sufficient security arrangements are in place to safeguard the data
- that the use will not be for purely commercial purposes

For more information visit https://digital.nhs.uk/

H WORKING WITH A NEW DATA SUPPLIER

When working with a new supplier of secondary data, there are a number of things you may want to check and clarify with them prior to starting a project.

Suppliers of secondary data for business intelligence provide information obtained from:

- Published data (e.g. provided by government departments of agencies such as patient level data from NHS Digital).
- Existing publications (e.g. news reports, scholarly articles, industry/consultancy reports).

Here's a checklist of things you might want to bear in mind along with your own specific requirements:

Contracts and permissions

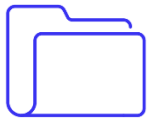
- Does your contract and Master Service Agreement cover any specific clauses relevant to the project requirements?
- If required, do you have proof from the supplier of any competency and compliance requirements?
- If you are sharing data you should check the redistribution rules within the terms of the agreement/contract. A Third Party Agreement (TPA) may be required.
- Check that you have the appropriate permission to use the data for the intended purpose under the terms and conditions of the contract or licence. If in doubt, contact the data owner for permission

Data Protection - additional checks that are recommended if the data you are receiving contains personal data

- Notify your Data Protection Officer (DPO) to ensure you understand any corporate requirements.
- Clarify respective roles and responsibilities - yours and your supplier e.g. data processing.
- Check that any personal data will be secure when being transferred and stored.
- Ensure you are aware of your legal basis for processing these data.
- Make sure that legal agreements between yourself and the supplier are in place.
    - If you are engaging a third party to process the personal data, ensure you have a contract stipulating compliance with your data protection requirements.
- Establish whether you will be required to remove, update or extract data from your systems in line with data subject requests.
- Ensure that your company's relevant privacy statements are amended to include the personal data you are being supplied.

The BHBIA has also produced a Due Diligence and New Technologies - Compliance: The New Normal guide (new in 2021) which suggests some helpful questions members can ask themselves when assessing new technologies e.g. file sharing technology or electronic signature software and doing their due diligence before using it on live projects – see the **Privacy & Data Protection** section of the website.

MANAGING DATABASES AND CRM



The key ethical and legal issues to be considered when managing or using databases are ownership of data / data structures and data protection considerations.

Regardless of the ownership of the database, any personal data contained within it will be subject to data protection law and all the considerations we've covered previously will apply. These key principles should also guide the use and storage of data within a CRM (Customer Relationship Management) system.

In particular, attention should be paid to make sure the database:

- Contains accurate and up to date personal data
- Does not contain more personal data than is required (principle of minimisation)
- Is hosted within the UK or European Union (EU) or other permissible states for data protection purposes
- Is only used for the purposes for which consent has been given, or for which an alternative legal basis for processing has been established
- Is kept securely with adequate controls to minimise the number of users with access to the personal data Where third party companies have access to the database, contracts must be in place with those organisations to ensure compliance with data protection law. Similarly, any third parties provided with personal data or able to access it through the database must do so under a contract covering their use of the data.

1 Ownership of data and data structures

Different aspects of databases are protected by two pieces of legislation:

- The Copyrights, Designs and Patents Act 1988
- The Copyrights and Rights in Databases Regulations in 1997

Copyright law protects the creative intellectual property (IP) involved in the data structures and presentation of the data within the database, while the Database Rights protect the investment that has gone into compiling the data itself.

The Owner of a database is the person or company who initially take the initiative in obtaining or verifying its contents:

- The Owner of a database can licence it to others, such as list providers, to use.
- When a database is used by someone else the Owner has the right to prevent the copying/restrict the use of substantial parts of the database by asserting their Database Rights, even if the data is transformed into a completely different structure by the user.

Creating your own database:

Where databases are created by company employees in the course of their employment, the company is considered to be the database Owner.

- In this case, Database Rights apply - the company does not need to apply or register for these – they are automatically credited to the Owner.
- The database may be shared with others outside the company, but you should ensure that an agreement is put in place to determine its use.

2 Appropriate data and use

When capturing data for storage and collection within a customer relationship management (CRM) system it's important to consider which data are appropriate

(Note: Although we refer here to CRM, similar considerations apply to separate account management systems, which often hold similar data.)

All users of the CRM should have training on the appropriate use of the systems and data before being provided with access - to ensure that only appropriate data are captured - and a training record should be kept as evidence. This should include organisational compliance aspects (e.g. what constitutes compliant practice for the company).

2.1 Personal Data

- Any data held within the CRM on Healthcare Professionals (HCPs) should be relevant to the business interaction.
- Hold only data necessary for the business practice and strictly no more.
- HCPs may give representatives their email addresses to enable an exchange of information, but this does not imply permission for the wider company to contact the HCP. A lawful basis for the use of this data for any other purpose must be established e.g. consent or legitimate interests.

Revised Guidance
Page 5

- The company must make sure that any personal data on HCPs or other customers held within the CRM is up-to-date and accurate, be this an in-house generated list or one purchased from a specialist list provider.
- Home address and other personal data about representatives irrelevant to their job should not be stored within the CRM system.

2.2 Free text

Free text fields within the CRM should be used sparingly, with caution, and for an appropriate and lawful purpose.

The main considerations are:

- ***Adverse Event reporting*** – ensure there is a mechanism in place to capture and monitor adverse events, product complaints and special reporting situations in the free text fields, and a procedure in place to ensure these are dealt with according to guidelines. You may decide to handle adverse events outside of the CRM to ensure compliance with PV guidelines including time to report an event.
- ***"Red-face test"*** – all information added to the CRM about an individual or organisation should be in reference to the business, accurate and written such that the company would be happy for the customer to see it if requested. e.g. when representatives capture the contents of the discussion and objectives for a next visit, they should be happy for this to be shared.

Individuals have the right to access all personal data related to them under data protection law.

2.3 Meetings & transfers of value

When meetings are planned, details of the expenditure and number of customers in attendance should be recorded (either in the CRM or another system) and signed off by a manager before the meeting commences. This is to ensure that the expenditure per head is within acceptable levels

- If transfers of value are recorded within the CRM system and these transfers of value need to be disclosed, please see the detailed guidance on disclosure within section E4.3 of the **BHBIA's Legal & Ethical Guidelines for Healthcare Market Research** (the BHBIA guidance relates to disclosure in the context of market research projects, but the same principles apply in other settings) and the **ABPI Code of Practice 2024** (clauses 28-31 deal with disclosure).

3 Storage and sharing of data

3.1 How should the data be stored?

Consider where the data are stored, as CRMs almost always contain personal data, which has to be protected under data protection law.

- Servers holding the system (and any record level analytics based on this data) should be located within one of the territories deemed to be adequate for data protection purposes, or contractual arrangements specifying security standards will need to be put in place.
- Field based devices enabling access to the CRM (laptops, tablets, smart phones) should have sufficient security protection to ensure the data is secure if the device is lost or stolen. Entry pins should be mandatory on mobile devices, and laptop hard drives should be encrypted.
- Data protection law requires that personal data is stored securely. Systems should be designed and developed with privacy requirements built in.

3.2 How can the data be shared?

Consider the following points about sharing data within and outside your company:

- Where companies are using medical (non-promotional) representatives (e.g. MSLs) and commercial salesforces, care should be taken to make sure that data entered into the CRM by the MSLs is not inadvertently shared with their promotional colleagues.
- If undertaking joint ventures, data will often be shared between the CRM systems of the interested parties. Be sure to inform your list provider that you are sharing these data before doing so, as there may be contractual obligations that need to be met or negotiated. It is also important not to share any personal data with the partner, such as representative names or address details.

- If asked to share information with an office based outside of the UK or European Union, make sure that adequate arrangements are in place to permit the transfer of personal data; alternatively supply anonymised or aggregated data only.

Check out the BHBIA's Sharing Personal Data – Quick Guide in the **Privacy & Data Protection** section of the website.

4 Measuring Sales Force Effectiveness

Clause 17 of the ABPI Code of Practice deals with representatives.

Analysts may work on Sales Incentive Compensation / Bonus schemes and need to be aware of:

ABPI Code Clause 17.7: *Representatives must be paid a fixed, basic salary and any addition proportional to sales of medicines must not constitute an undue proportion of their remuneration.*

Analysts may be involved in monitoring representatives' activity.

ABPI Code Clause 17.3, supplementary information deals with Frequency and Manner of Calls on Doctors and Other Prescribers.
Key points:

> *The number of calls made on a doctor or other prescriber by a representative each year should not normally exceed three on average. This does not include the following which may be additional to those three visits:*
> *• attendance at group events/meetings, including audio visual presentations and the like*
> *• a visit which is requested by a doctor or other prescriber or a call which is made in order to respond to a specific enquiry*
> *• a visit to follow up a report of an adverse reaction.*
>
> *When briefing representatives, companies should distinguish clearly between expected call rates and expected contact rates. Contacts include those at group events/meetings, visits requested by doctors or other prescribers, visits in response to specific enquiries and visits to follow up adverse reaction reports. Targets must be realistic and not such that representatives breach the Code in order to meet them.*

Follow up studies of representatives' visits

Typically, this market research process involves recruiting doctors (or other HCPs) from a call list supplied by the commissioning company. Doctors that a sales rep recently visited are interviewed to assess their recall and the impact of both the visit and the sales material.

Client company analysts may be asked to provide contact lists for this purpose.

Under data protection legislation:

- researchers using lists must have a lawful basis for the use of any personal data
- the agency must be under contract to the client, working as their agent to ensure protection of the data
- you need to ensure that there is a third-party agreement or non-disclosure agreement in place and adequate consent has been established if the client company leases it lists from a data supplier
- the agency must not add the data to any of its own databases without obtaining the respondents' permission beforehand
- the agency should destroy the sample lists or return them to the client at the end of the project

J MANAGING CONSENTS

Consent gathering is often an essential feature of modern sales and marketing effectiveness strategies

GDPR/DPA 2018 has forced consent into the spotlight and now customers (in our case HCPs and other healthcare system stakeholders), are much more aware of their right to opt out as much as their right to opt into a company's promotional messages, channels and content.

1 Before you commence

As a first step we recommend that you audit your company's data and processes:

- **Audit the data already on file, in your CRM (or equivalent) system:**
    - How up to date is it?
    - Where did it come from?
    - Who has it been shared with, who will you share it with for the approved purposes?
    - Was it collected for a specific purpose, is this relevant going forward?
    - Were the respondents notified of their rights at the time?
- Have you identified a lawful basis for processing this data?
- How ready are your systems - CRM, Data Warehouse, Analytics, MDM (Master Data Management) - to handle a compliant consent approach?
- How well are you able to manage the consents data? (for example locking down the ability to extract and store consents, being able to provide a "consents coverage" report to monitor uptake)
- Are your field and Head Office teams "consent ready" in terms of their knowledge and levels of training?
- Are you 'audit ready'? Have you conducted a mock audit in case of a real audit or data breach?

2 Gathering consents

The purpose of consent must be specific.

Some companies are gathering consents by content type - e.g. promotional, scientific, disease awareness, company related, meeting related **and by channel** - e.g. SMS, E-mail, direct mail, CLM, Remote Meeting, Webinar/webcast

When building your capability to gather consents, bear in mind that you'll need to be able to allow individuals to withdraw their consent as easily as they gave it, if they want to do this, and within the required timescale, with proof available.

Here are some top tips:

- **Agree with your senior management the principles and parameters**. For instance, will your consent functionality promote best practice or actively "police" inappropriate communication without consent?
- **Seek a clear and active opt-in** such as unticked opt-in boxes or similar active opt-in methods (make it easy for your field teams to build consent capture into an interaction).
- **Consider, share and remember the advantages** of gathering consent for your business operations and your customers (compliance, communications, consistency).
- **Avoid making consent a precondition of service.**
- **Be specific and granular**. Allow individuals to consent separately to different purposes and types of processing wherever appropriate - but don't over-complicate the process.
- **Name your business and any specific third-party organisations who will rely on this consent.**
- **Keep records of what an individual has consented to**, including what you told them, and when and how they consented. This will help when auditing and responding to customer requests.
- **Tell individuals they can withdraw consent at any time, and how to do this.**
- **Include a way of getting the privacy notice to the customer**, perhaps as part of an automated receipt process.
- **Test the processes extensively from end to end** – meaning from the initial gathering through to opting out and recording such decisions.

3 Storing consents and managing requests

Storage should follow the GDPR/DPA 2018 principles including relevance, appropriateness, security and transparency.

- Data transfer should be kept to a minimum and be justified where used.
- The fewer places the data is held then the easier it is to manage.

Customers now have a legal right to be able to access their personal data held on the company's CRM system (and other downstream or upstream systems).

- Is there a clearly defined process in place for customers to request and receive their data?
    - It should also cover supplementary information e.g. notes held against the customer's name following a call, or pre-planning notes that are specific to that customer in the CRM system.

Customers can request information in writing or verbally, all customer facing teams should be ready to deal with this in a prompt manner.

- Fees can only be charged if the request is "manifestly unfounded or excessive, particularly if it is repetitive; or for further copies of the same information (that's previously been provided)" – Information Commissioner's Office (ICO).

> **Important distinction** – under GDPR/DPA 2018 you need to gather and manage separate consent for "automated profiling" as a type of data processing. Many "AI" type solutions utilise algorithms that automatically learn, process and predict outcomes or next best actions based on data lakes. It is precisely these types of applications, which are linked to CRM and Analytics systems, that this condition refers to, so be wary of this.

4 Ongoing consent management and review

Obligations don't end when you first get consent.

There are a range of different approaches and pre-conditions built into CRM systems which companies use for consent management.

- Some are iPad or tablet centric which makes it very easy for Reps and MSLs to build the consent capture into an interaction.
- Be careful to balance the ethical baseline requirements with making this an easy operation for your field teams and customers. Don't over-complicate based on CRM functionality "because it can".

Ensure that consents gathered via CRM are managed alongside other channels.

- Other channels which gather consent might include HCPs at a conference consenting on paper or a "privacy portal" where customers can opt-in and out dynamically.
- Work with your compliance and legal colleagues to ensure that these methods are all compliant and, importantly, linked up to preserve the "single version of the truth".

Does the data need to be transferred from one system/location to another?

- Are the necessary NDAs (non-disclosure agreements) and privacy protections in place?
    - If you are transferring consent data, make sure that the relevant processes and safeguards are used - e.g. encryption of the data. Use pseudonymisation or anonymisation of data whenever practical.

Keep consents under review and update them if anything changes.

- Refresh consent on an ongoing basis, it is not a one-off compliance box to tick and file away. Your CRM consent should always reflect the latest status.
- Set a time limit for how long you should keep the data. You should have a system or process to capture these reviews and record any changes.
- Some companies use hard copy mailing alongside electronic methods to review consents. An audit trail should be kept.
- Maintain a dialogue with Compliance, Legal and Marketing to keep pace with legislative changes and commercial initiatives that may require customer consent.
- Review your privacy notices annually to make sure they're still relevant and importantly in line with data privacy law.

5 Opt-outs and records management

Customers can request to be opted out of either commercial databases and/or your own company processing

- This includes internal databases including data warehouses and CRM.
- Ensure you have a process, with audit trail built-in, to keep a record of when, where and how the opt-out was fulfilled.
- These can be “soft opt-outs”, as it may be the case that your sales or medical colleagues will wish to restore the customer’s record in your systems if and when there is agreed value in doing so. Obviously, this can only be reinstated with an auditable request coming directly from the customer.

Ensure your CRM database solution has facilities to manage the following, with an audit trail built in:

- Opt customers out of processing by your company (in this case they may wish to stay in the industry database or opt-out altogether).
- Opt customers into processing by your company (they may have chosen to opt out of the industry databases but wish to stay connected with your organisation).
- Opt the opted-out customers back into processing should their preferences change in the future.

An important consideration is to actively manage the customer’s record’s footprint and “breadcrumb” their profile within your company.

- There are likely to be several records held across systems, databases and physical / logical systems of the same customer.
- These records need to be actively managed and a process for systematic cleansing of such records implemented and enforced.
- Without having an active process in place that checks folders, sharepoint sites, local and network drives for outdated customer extracts, you will be running a risk of customer records becoming active inadvertently and the opt-out request becomes invalid.

This is a key opportunity to implement housekeeping processes with auditable implications and hence raise the profile of the data steward role internally as well as presenting a professional GDPR compliant interface externally.

K ARTIFICIAL INTELLIGENCE AND DATA PROTECTION

Revised Guidance
Page 5

1 Introduction & key principles

Because of the way it is likely to be analysed and processed Data generated from or analysed through Artificial Intelligence (AI) needs special legal and ethical considerations

Artificial Intelligence - General principles

A review of the information collected should be conducted to determine whether it contains any personal data - if so data protection principles apply.

- By definition, data that is generated from Artificial Intelligence and containing personal data is likely to be considered a high-risk asset due to the artificial manner of its collection and the high impact of any breach or misuse of such data.
- Higher standards and risks will apply if these data sets contain special category (sensitive) personal data
- Consider whether it is necessary to be able to identify individuals from the data. If not, e.g. if the data is being used for general analysis of populations or cohorts, then anonymising the data will remove it from the scope of data protection requirements

Processing Data gathered via AI and containing personal data can provide challenges under some of the data protection principles which we will go on to consider.

What is Artificial Intelligence (AI)?

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think and learn. AI encompasses a variety of technologies, including machine learning, natural language processing, and computer vision, which enable machines to perform tasks that typically require human intelligence.

Generative AI is a subset of AI that focuses on creating new content, such as text, images, audio, and video, from existing data. Generative AI models are trained on vast amounts of data and can generate human-like text or realistic images based on given prompts.

AI Legislation and Regulatory Advice:

The **EU AI Act** is a regulatory framework approved by the European Union to ensure the safe and ethical use of AI. It is important to note that the EU AI Act is European legislation and does not directly apply to the UK. Nonetheless, it provides a useful framework for understanding and managing AI risks. It is worth noting that the ICO, who advise on AI use in the UK to the UK Government, references the four risk categories below.

It is also worth noting that if any of the outputs of the data analysis are used outside of the UK, and within the EU, then EU AI Legislation will apply.

The EU AI act classifies, and ICO references the same, AI systems into four risk categories:

- **Unacceptable Risk**: AI practices that pose a clear threat to safety, livelihoods, and rights, such as social scoring by governments, are prohibited.
- **High Risk**: AI systems that affect safety or fundamental rights, such as biometric identification and critical infrastructure, are subject to strict regulations.
- **Limited Risk**: AI systems with specific transparency obligations, such as chatbots, must inform users they are interacting with AI.
- **Minimal Risk**: All other AI systems, which pose minimal or no risk, are subject to limited obligations.

Most market research uses of AI will fall into the **minimal or limited risk categories**, as they are unlikely to involve automated decision-making or processing of personal data related to fundamental rights. This means that in many cases using AI to process data will have similar implications as processing data using traditional data analysis techniques.

AI and Consent

If AI is used solely to process or analyse anonymized or pseudonymised data in a secure environment, it does not necessarily require specific AI consent (e.g. in a screener) as long as the data is only used for the purposes for which the respondent has given their consent. However, as AI is a new and rapidly evolving technology, consider whether it

would be valuable to provide transparency on your use of AI with the respondent by including mention of AI use in the screener.

Ethical Principles Covering AI

The usual principles of ethical data use apply to AI, including:

- **Data Minimization**: Only collect and process the minimum amount of data necessary for the research purpose. When using AI, ensure that the data inputted is relevant and limited to what is needed.
- **Consent**: Obtain informed consent from respondents, clearly explaining how their data will be used. Stipulating that AI will be used to process a respondent's data is not necessarily needed – however, consider whether it would be valuable to provide transparency on your use of AI with the respondent depending on the use case.
- **Transparency**: Be transparent about the use of AI in the research process. You may want to inform respondents and clients about how AI Some key tools will be used to ensure they are not mistaking an AI produced output for a real image / case study, for instance. Be mindful of any provisions in client contracts that would require this level of transparency.
- **Accountability**: Ensure clear lines of accountability for the use of AI tools. Designate responsible individuals or teams to oversee AI processes and ensure compliance with ethical and legal standards. Consider establishing a formal AI governance committee and policy or incorporating AI governance principals into existing corporate policies.
- **Bias and Fairness**: Be aware of the potential for biases and inaccuracies in AI-generated outputs. Ensure that AI tools do not perpetuate stereotypes or inaccuracies, particularly in sensitive areas like patient research.
- **Human Oversight**: Maintain human oversight throughout the AI processes. Researchers should review and validate AI-generated outputs to ensure accuracy and relevance; researchers ultimately remain solely responsible for the quality of their work. Ensure that human users of AI tools have received adequate training.

Assessing AI Tools

When assessing whether to use AI tools, consider the following:

- **Data Privacy and Security**: Ensure that the AI tool complies with data protection regulations, including GDPR. If personal data may be inputted into the AI tool, verify that the tool has robust security measures to protect the data.
- **Data Retention and Usage**: Confirm that the AI tool does not save personal data or use it to train future models. This is crucial to prevent unauthorized use or exposure of sensitive information.
- **Vendor Assessment**: Conduct thorough assessments of AI tool vendors, including their compliance with data protection laws, security measures, and transparency about their algorithms and data sources.
- **Data Protection Impact Assessments (DPIAs)**: For AI tools consider DPIAs to identify and mitigate potential data protection risks.
- **Meeting ICO Expectations**: Ensure that use or integration of an AI tool allows your organization to remain compliant with the ICO's advice and expectations for the use of AI systems.

2 Transparency and purpose of processing

Some aspects of data protection law create challenges for Artificial Intelligence, if it contains personal data.

The 'fair and lawful' principle:

Data subjects have the right to know what their data is being used for.

- The complexity of artificial intelligence/machine learning makes it difficult to provide an easy to understand description of the processing.
    - It is important that processing is in line with the details provided in privacy notices and What the data subject would reasonably expect their data to be used for.

The purpose of processing:

AI offer massive diversity in their potential uses. However, just because an analysis is possible in the data, this does not mean that there is an automatic right to perform it.

- Where consent is the basis for processing, it must be established whether any new use of the data is still covered by the original consent given.
- Where a legitimate interest of the organisation is used as the legal basis, there is a responsibility to assess the data use and ensure it is respectful of the rights and interests of the data subjects.
- Where data is purchased from a third party and integrated with other Big Data, there is still a responsibility to ensure the data is used in accordance with the purposes set out in the third party's privacy statement.

3 Specific challenges

3.1 Complexity

- Under the data protection law, data subjects have the right not to be subjected to fully automated decision making where the outcome has a material (e.g. legal) impact on them.
- Therefore, the data controller must ensure that appropriate techniques are applied accurately, and that they could not lead to discrimination based on special category data factors (e.g. race, health etc.).
- When consent is provided by individuals, the automated decision making needs to be as anticipated by the subjects.
- If for example patient datasets are being analysed, the algorithms to model and analyse the data sources need to be documented. If the algorithm is being changed, this needs to go through a new round of review and approval.
- But in case of machine learning to model the data, it is not exactly known anymore how the algorithm makes and evolves its determinations. It is also not possible to control or advise when it changes, as this is part of the process of continuously testing and improving the model. This is in fact the very essence of machine learning (continuous iteration and improvement) but is by nature difficult to document and maintain.

3.2 Data accuracy

- Data protection law requires that data being kept is accurate (as far as possible).
    - This is especially important in the case of automated decision making in subgroups, where data accuracy can be lower than in the overall population.
    - This can be a challenge with Big Data, not only because of the volumes involved, but also because there is often less validation built into its collection. Data subjects may provide false information as a means of protecting their privacy, or more inaccuracy may be tolerated in the data as it is thought that the size of the dataset will marginalise incorrect data.
    - Particular attention should be given to data modelling and machine learning techniques based on whole populations, where inaccuracy in the model may be biased towards subsets of the population (e.g. the model is 95% accurate for the population, but only 50% accurate for a particular minority). This can cause “unfairness” in the decisions made as described above. Where possible, make machine learning algorithms auditable and check them for bias. Similarly, care should be taken when interpreting outcomes derived from complex algorithms on Big Data to determine whether they represent causal insights or merely correlation of factors.

3.3 Feasibility and quality

- Depending on the data that are being used, data privacy can have an impact on the feasibility of the Artificial Intelligence activity and/or adversely affect a company’s opt-in rates (consents).
- At the same time, it can build trust with internal/external stakeholders and increase the quality of the data sources/outcomes of an AI project.

3.4 Adequacy of data (data minimisation) and retention

There is often a tendency with AI Data to collect as much information as possible, and from an AI perspective the more data the better, but with personal data, organisations have a responsibility to process and store (including in backups) only the data necessary for the specified purpose.

- If personal data is required in the data, consider whether there are aspects that are not needed (e.g. date of birth might be stored where year of birth could be adequate).
- Reducing the data stored to the minimum required can also help with data volumes and processing speeds and costs.
- There is always an argument to hold on to data and to build up a historical catalogue, but under data protection legislation, data subjects need to be told how long their data will be stored for, and in most cases the data must then be deleted, however valuable.

3.5 Security and location of processing

Due to the processing power required to manage AI Data processes, Cloud based computing is often used.

- Risk assessments should be performed to ensure the security standards met by any such third party are adequate. Various internationally recognised standards can help assess this, such as ISO 27001 (information security), ISO 14644 (data centre cleaning), ISO 9000 (Quality).
- The location of the data centre, as well as any backups or failover systems should also be considered, as there are legal complications if the personal data of UK or European citizens is processed outside of the UK/European Economic Area.

4 Adverse Events, Product Complaints and Special Reporting Situations

4.1 Overview

Marketing Authorisation Holders (MAHs) for medicines and Certificate of Conformity holders for medical devices have a legal and regulatory obligation to monitor, collect and manage adverse events, to fulfil their product safety responsibilities

There are three types of events that need to be considered (Sometimes, 'adverse event' is used as an umbrella term intended to encompass all three types of event).

1. **Adverse Event (AEs)**
2. **Product Complaints (PCs)**
3. **Special Reporting Situations (SRSs)**

See section M for full definitions of each of these types of event.

Please refer to the ABPI/BHBIA ***Guidance notes on collecting adverse events, product complaints and special reporting situations during market research*** in the Guidelines and Legislation > Adverse Event Reporting section of the BHBIA website. The guidance notes were updated in February 2021 to include medical devices as well as medicinal products.

See also: ABPI *Guidance notes on the management of safety information and product complaints from digital activities*

Hereafter, we will use the abbreviations AE, PC and SRS.

The management of AEs, PCs and SRSs found in Artificial Intelligence does not fundamentally differ from those found in other ways, but AI is one area where analysts may be particularly likely to come across them.

- Any AEs, PCs or SRSs identified during an AI project (carried out by or for the MAH) need to be processed.
- When working with the amount of data required for AI, a lot of AEs, PCs and SRSs could be hidden in the files. So, you need to ensure they are captured. AI itself could be the best way to identify them in the data (for example using pattern or text recognition).

(Internet or Digital Media need to be actively screened on a regular basis anyway, if it is under the MAH's management or responsibility.)

4.2 Planning a project

Before starting an AI project, it is important to discuss the potential to generate AEs, PCs and SRSs with the relevant company functions like pharmacovigilance, compliance, legal, etc.

In these discussions:

- Be realistic about the number and kind of events that could be found, so that the additional workload doesn't take people by surprise.
- Decisions need to be made on how AEs, PCs and SRSs are going to be monitored and processed and how the AE/PC/SRS reconciliation at the end of the project will be managed. For large numbers of AEs/PCs/SRSs, reporting them in table format can be more practical, but keep in mind some companies or departments insist on receiving them on a (case by case) reporting form.
- Ensure that clear roles and responsibilities are assigned.

The requirement for AE/PC/SRS reporting can have an impact on the feasibility of the Artificial Intelligence activity, but at the same time it can build trust with stakeholders and increase the quality of the outcomes.

4.3 Responsibilities and training

Don't forget that all staff members involved in the AI project that can potentially identify an AE, PC or SRS need to be properly trained, which includes agency personnel, and ensure that records of the training are kept.

- The BHBIA provides an **online training programme** ***Adverse Event Reporting in Market Research*** that covers core requirements. Completion of company-specific training may also be required.
- Specifically, ensure staff are aware that AEs, PCs and SRSs need to be reported even if a **group of patients** was mentioned, rather than an individual (as long as it is a particular group of *actual* patients, whether or not specific identifiers are available).
- Also ensure they are aware that **off-label usage or lack of efficacy** of one of the MAH's products (both of which could be very common), need to be reported as these are Special Reporting Situations.
- **If an external vendor is involved in AI,** a contract needs to be in place clarifying responsibilities in terms of AE/PC/SRS management.

Further Reading:

- MRS Guidance on Using AI Related Technologies – updated April 2025
- MRS Clientside Best Practice Guidance – Client Perspective on inclusion and AI – updated July 2025

L APPENDIX

DATA PROTECTION LEGISLATION

FOR DETAILED ADVICE AND EXPLANATIONS OF DATA PROCESSING REQUIREMENTS PLEASE SEE THE PRIVACY & DATA PROTECTION PAGE ON THE BHBIA'S WEBSITE.

1 Personal data, health data and data processing

The GDPR defines personal data as

> "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

Personal data that has been pseudonymised falls within the scope of the data protection requirements. If you have the means to reverse the pseudonymisation within your organisation, the pseudonymised data must be treated as personal data.

Personal data includes electronic, manual and recorded data held in alphabetical, numerical, graphical, photographical or acoustic form. Audio that could identify an individual and image data also qualify. Personal data may be a single piece of information or a series of pieces of information which together allow identification of an individual.

Once data has any identifiers linking it to a natural person removed, it's no longer personal data or covered by the Act. However, you must make sure that de-identified data cannot be traced or an individual's identity inferred by deduction.

- Special category (previously referred to as sensitive) personal data

  This includes information about race or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, offences commissioned or carried out, whether alleged or committed. The definition of health data has been expanded to include biometric and genetic data.

  You must obtain explicit consent to process special category personal data. You must treat special category personal data with greater care than other personal data.

- Processing

  You must process personal data in accordance with the Data Protection Act including: collecting, recording, organising, storing, altering, retrieving, using, disclosing, disseminating, aligning or combining, blocking, and erasing or destroying.

- Health data

  Under the UK GDPR, 'data concerning health' means personal data related to the physical or mental health of a natural person. This definition includes the provision of healthcare services, which reveal information about a person's health status. The Information Commissioner's Office (ICO) has confirmed that 'data concerning health' can also relate to healthy individuals, and includes data from medical devices and fitness trackers (e.g. the number of steps taken by the user or athletic performance). Data such as appointment details, reminders and invoices may also constitute health data if it reveals or could in combination with other data reveal information about a person's health through 'reasonable inference'.

  Additionally, the UK GDPR uses the concepts of 'genetic data' and 'biometric data'. 'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or the health of that natural person. Such data results, in particular, from an analysis of a biological sample from the natural person in question. 'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person. Biometric data is an open category and can include a broad set of identifiers such as DNA matching, iris and retina recognition, facial recognition, and fingerprint and voice recognition.

Source: *Lexology: At a glance: data protection and management of health data in United Kingdom*

2 Requirements, roles, responsibilities and key principles of data processing

You must make sure that your work conforms to the UK Data Protection Act 2018 and UK GDPR.

- Responsibilities

  The UK Data Protection Act 2018 is administered and enforced by the independent Information Commissioner's Office.

  Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

  Article 5(1) requires that personal data shall be:

  > "(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
  >
  > (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
  >
  > (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
  >
  > (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
  >
  > (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
  >
  > (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

  Article 5(2) adds that:

  > "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

  See For more information on key principles, visit the **Information Commissioner's Office (ICO) website**. The ICO is the UK's data protection regulatory body.

- Data processing

  'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- Controller and processor roles

  A data controller is a person who (either alone or jointly or in common with others) determines the purposes for which and the manner in which any personal data are, or will be, processed. Data Controllers must pay a notification fee to the ICO.

  A data processor is any person (other than an employee of the data controller) who processes data on behalf of the data controller. For example, any contractor who processes data on the controller's behalf.

  Controllers must only use processors which are able to guarantee that they will meet data protection requirements and protect the rights of data subjects.

Whenever a controller uses a processor there must be a written contract in place. Similarly, if a processor employs another processor it needs to have a written contract in place. The contract must state details of the processing and must set out the processor's obligations. This includes the standards the processor must meet when processing personal data and the permissions it needs from the controller in relation to the processing.

The ICO advises that contracts must set out the:

- subject matter and duration of the processing; the nature and purpose of the processing;
- type of personal data and categories of data subject; and
- obligations and rights of the controller.

Contracts must also include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights;
- assist the controller in meeting its data protection obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their obligations, and tell the controller immediately if it is asked to do something infringing data protection law .

Your processor should not employ another processor without your prior specific or general written authorisation. Sub-processors do not have to be named in contracts as the list of sub-processors is subject to late changes or changes mid-project so it's not practical to name all individuals/organisations and it is sufficient to name types of sub-processors (e.g. recruiters, interviewers). If a processor employs a sub-processor, then it must impose the contract terms on the sub-processor.

For further details see *ICO GDPR guidance: Contracts and liabilities between controllers and processors*

- Data Protection Officer (DPO)

DPOs are required for organisations whose core activities involve:

- either regular and systematic monitoring of data subjects on a large scale or
- large scale processing of special category data and data relating to criminal convictions.

Appointment of a DPO is likely to be a requirement for some MR suppliers. For further information about appointment of DPOs see the BHBIA's *Data Protection Officer* guide in the **Privacy & Data Protection** section of the website.

ADVERSE EVENTS, PRODUCT COMPLAINTS AND SPECIAL REPORTING SITUATIONS – DEFINITIONS

FOR FULL DETAILS PLEASE SEE THE **ADVERSE EVENT REPORTING** PAGE ON THE BHBIA'S WEBSITE.

1 Adverse Event

An adverse event (AE) *is 'Any untoward medical occurrence in a patient or clinical trial subject administered a medicinal product and which does not necessarily have to have a causal relationship with this treatment.*

An adverse event can, therefore, be any unfavourable and unintended sign (e.g. an abnormal laboratory finding), symptom or disease temporarily associated with the use of a medicinal product, whether or not considered related to the medicinal product.'

Adverse events may be associated with medical devices too. In this case, 'adverse event' means any untoward medical occurrence, unintended disease or injury or any untoward clinical signs, including an abnormal laboratory finding, in subjects, users or other persons, whether or not related to the device.

Where it is reasonable to consider there is a ca l relationship between a medicinal product or medical device and an AE (i.e. that the medicine or device is contributing to causing an AE), and the response to the medicine or device is noxious and unintended, the AE is known as an 'adverse drug reaction' or an "adverse incident" in the case of medical devices

2 Product Complaint

A product complaint (PC) is any alleged failure of a medicinal product or medical device, including identity, durability, reliability, safety, efficacy or performance. It is specific to the medicine or medical device itself or its packaging, as opposed to its effect on the patient.

For example:

- Damaged or missing tablets
- Incorrect strength, marking or colour of tablets
- Damaged packaging
- A label that cannot be read
- A liquid that should be clear but is cloudy or contains unexpected particles
- A bent needle
- A broken syringe
- A missing patient information leaflet
- The identification of a potentially counterfeit medicine or medical device
- A malfunction of the device

3 Special Reporting Situation

The following are **all special reporting situations (SRSs):**

- Exposure through a parent i.e. medicine exposure to a foetus in utero (whether the foetus is exposed because the mother took the medicine during pregnancy or transmission from semen following the father's exposure to the medicine)
- Use of a medicinal product or device during pregnancy or breastfeeding
- Reports of overdose, abuse, misuse
- Lack of therapeutic efficacy including suspected use of counterfeit/falsified medicines/tampering
- Medication errors (including dispensing errors, accidental exposure, maladministration etc.)
- Unapproved, or off-label use of a medicine or device i.e. intentional medical use that doesn't comply with the authorised medicine or device information (including off-label use in children or the elderly)
- Withdrawal symptoms syndrome

A company may also indicate to the MRA that it considers the following to be an SRS and the MRA should make sure it understands exactly how the company defines this:

- Unexpected therapeutic benefit (the pre-existing condition improved)

Please also send the MAH/Certificate Holder any information received relating to these safety situations:

- Medicine or medicine-food interactions
- Suspected transmission of an infectious agent

Occupational and environmental exposure (as a result of a professional or non-professional occupation

Reference: ABPI/BHBIA **Guidance notes on collecting adverse events, product complaints and special reporting situations during market research**

COMPLAINTS POLICY

The BHBIA can only engage with complaints that relate to either:

1. **A potential breach of BHBIA Guidelines[1] committed by a current BHBIA member[2] organisation / individual, or their subcontractor when conducting business intelligence[3] activities in the UK[4]**
2. **A service provided by the BHBIA - e.g. an event or resource - or an interaction with one of the BHBIA team**

The complaints policy is open to any individual or organisation who has a complaint which meets the above criteria (referred to hereafter as the 'complainant').

To help us respond to your complaint:

- Please provide us with as many specific details as possible about your concerns – i.e. the exact nature of the complaint(s) and the details of the individual/organisation you are complaining about (referred to hereafter as the 'complainee') – for example, organisation name / individual name / project reference no. etc. as applicable.
- Unless specific circumstances make this difficult, this information will be required in writing.
- Complaints will be initially investigated by the BHBIA's administrative staff and contracted independent support team, including as appropriate, the BHBIA's Officer(s) and/or the BHBIA's Ethics Advisor. If it is necessary to seek wider opinions, it is likely that appropriate members of the BHBIA Board or Ethics & Compliance Committee (ECC) will become involved.
- In the interests of transparency, and to give the complainee a fair opportunity to respond to the specific issues, we will normally only consider a complaint if you consent to your identity being made known to the complainee; however there may be exceptions to this and if you have a clear justification for remaining anonymous we will consider it.
- Beyond the above, your identity will be kept confidential and only shared with members of the contracted independent support team directly involved in investigating the complaint. Likewise, the identity of the complainee will also be kept confidential.
- Should the investigating team be extended to Board or ECC members, identifying details of the complaint, including the individuals and organisations involved (both complainant and complainee) will be anonymised.
- Any complainant will be expected to attempt to resolve the matter with the complainee before approaching the BHBIA. We may ask you to satisfy us that you have taken all reasonable steps to try to do this, before coming to us
- We will not usually be able to engage in discussions about a complaint if there are legal proceedings contemplated or ongoing in respect of the matter
- Please ensure that you make it clear to us whether you are letting us know about a situation for information purposes only, or whether you are specifically asking us to investigate a complaint

Please note that unless there are exceptional circumstances we cannot consider a complaint that's more than 3 months old (i.e. more than 3 months has passed since the behaviour / action that you are complaining about).

Our commitment to you – we will:

- Take your concerns seriously and make every effort to help resolve them constructively, impartially and efficiently
- Acknowledge receipt of your complaint within two business days and provide a contact name in the BHBIA team for you to communicate with
- If we cannot resolve the issue straight away, keep you updated on progress
- Should the investigating team be extended to the Board and no resolution is found, the Board has the power to enact clause 15 – Expulsion of Member as outlined in the Articles of Association

To submit a complaint please fill in a contact form here: **https://www.bhbia.org.uk/about-us/contact** or call us on 01727 896085.

This Complaints Policy can also be found online on the BHBIA website at: **https://www.bhbia.org.uk/about-us/legal-financial-policies/bhbia-policies**

References

[1] BHBIA Guidelines includes the BHBIA's *Legal and Ethical Guidelines for Healthcare Market Research* and *Legal and Ethical Guidelines for Healthcare Data Analytics*, and the ABPI/BHBIA *Guidance notes on collecting adverse events, product complaints and special reporting situations during market research.*

[2] BHBIA member companies include full members: corporate, affiliate and personal and certified non-members: corporate and personal. Companies that are sub-contracted to a BHBIA member company for a business intelligence project are also required to follow the guidelines, so would be covered by this policy, with the member company ultimately being responsible.

[3] Business Intelligence activities include, but are not limited to: primary market research, secondary data collection and analysis, syndicated data services, field force effectiveness services and fieldwork recruiting.

[4] The BHBIA guidelines only cover work conducted in the UK, however it does not matter where the member organisation or individual is based.

KEY TERMINOLOGY

Agency Any individual, organisation, department or division, (including any belonging to the same organisation as the client) that is responsible for, or acts as, a supplier on all or part of a project.

Anonymisation The process of removing, obscuring, aggregating or altering identifiers to prevent identification, using reasonable means, of the individuals to whom the data originally related.

Anonymity Non-disclosure of identity.

Anonymous data Data that does not relate to an identified or identifiable individual, the data subject is no longer identifiable. Anonymous data is no longer personal data.

Client Any individual, organisation, department or division which requests, commissions or subscribes to all or part of project.

Consent The freely given specific and informed agreement by a person (i.e. the 'data subject' or 'respondent') to the processing of their personal data.

Consultant Any individual or organisation that provides business intelligence services, including subcontractors.

Data controller alone or jointly with others, determines the purpose and means of the processing of personal data.

Data processor processes data on behalf of the data controller.

Data subject A living identifiable person on whom personal data is held.

Digital listening Extracting data from social media for secondary analysis (e.g. sentiment analysis), automatically or manually.

Explicit consent Although not clearly defined within the GDPR it is basically a slightly higher standard of consent and is necessary for (amongst other things) processing special category (sensitive) personal data such as health data. Explicit consent must be confirmed in a clear and specifically worded statement (oral or written), so signing a statement would be explicit consent but an affirmative action alone such as responding to an email requesting consent would not be explicit consent.

Healthcare organisations include a healthcare, medical or scientific association or organisation such as a hospital, clinic, foundation, university or other teaching institution or learned society whose business address, place of incorporation or primary place of operation is in Europe or an organisation through which one or more HCPs or other relevant decision makers provide services.

Healthcare professional (HCP) Any licensed member of the medical, dental, pharmacy or nursing professions or any other person who, in the course of their professional activities, may administer, prescribe, purchase, recommend or supply a medicine. The ABPI definition of HCP also includes: officials or employees of government agencies or private or public sector organisations that may administer, prescribe, purchase, recommend or supply medicinal products. The ABPI refer to 'other relevant decision makers' as including those with an NHS role who could influence in any way the administration, consumption, prescription, purchase, recommendation, sale, supply or use of any medicine but who are not HCPs.

Non-HCP could include a patient, sufferer, carer, family member, member of the public, journalist.

Identity Information, as well as the name and/or address, from which recipients might identify respondents.

Market research Market Research (MR) whatever it is called, whoever commissions it and whatever approach is used, has four key characteristics: 1. Its purpose is to gain insight or support decision making by generating understanding and knowledge. 2. It involves the systematic collection, analysis, interpretation and use of information about individuals, organisations or market places using the information gathering and analytical methods and techniques of the applied social, behavioural and data sciences, statistical principles and theory. Information (data) is obtained from specific samples and the findings extrapolated to the population as a whole. MR is scientifically conducted. 3. MR has no interest in the individual identity of respondents; respondents have to be offered confidentiality and anonymity even if we then ask them to waive it e.g. so that we can view non-anonymised fieldwork. 4. It does not result in direct action relating to individuals or organisations participating in it (except following up adverse events when permitted). MR is not a commercial communication or a selling opportunity.

- **Primary market research** generates original data directly from respondents to solve the problem in hand. Primary data is derived from new and original research designed to address a specific purpose.
- **Secondary market research** Data already collected for one purpose is then re-analysed for another.

Masking Altering original social media data (e.g. comments, photos or videos) to a point that it cannot be traced back or attributed (e.g. using a search engine) to the original user.

NDA Non Disclosure Agreement. Also known as a confidentiality agreement, this is a legal contract or part of a contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to.

Passive social media monitoring Extraction of data from social media for analysis where there is no interaction with the contributor. Also known as digital listening or scraping.

Patient organisation means an organisation mainly comprised of patients and/or caregivers or any user organisation such as disability organisation, carer or relative organisation and consumer organisation that represents and/or supports the needs of patients and/or caregivers.

Personal data Any information relating to an identified or identifiable living person, who can be identified directly or indirectly by that data on its own or together with other data.

Privacy notice/policy is a published summary of an organisation's privacy practices, it describes the ways in which the organisation gathers, uses, discloses, transfers and manages a data subject's personal data.

Processing of personal data Any operation or set of operations performed on personal data, including, but is not limited to: collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, blocking, erasing or destroying, whether automatically or otherwise.

Profiling Means any form of automated processing consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects of the individual's performance, preference, behaviour or health.

Promotional or sales activities Designed to change consumers' attitudes towards products or services in order to encourage them to buy or take these up.

Pseudonymisation This means the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject e.g. all identifiers have been removed and are stored separately. If the means to reverse the pseudonymisation are available within an organisation, the pseudonymised data is still classed as personal data.

Public domain Information, which is published and generally accessible or available to the public. Content that no one owns or controls, with intellectual property not protected under patent or copyright. In the business intelligence context it refers to information that is freely available, without restriction.

Public relations activities Designed to enhance public perceptions of bodies, organisations, etc.

Scraping Extracting data from social media for analysis, either automatically or manually.

Social media data Information (photos, comments etc.) that users generate or share while engaged in or with social media. It often includes personally identifiable data.

Special category data reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Subcontractor An individual or organisation that undertakes a part of a project under the instruction of the lead agency (the contractor).

Transparency Ensuring individuals have a very clear and unambiguous understanding of why the data is being collected and how it will be used.

SOURCES AND FURTHER READING

Our guidelines draw on the following sources.

1 Primary sources

BHBIA:

Privacy & Data Protection guidance

Legal and Ethical Guidelines for Healthcare Market Research

ABPI/BHBIA Guidance notes on collecting adverse events, product complaints and special reporting situations during market research

Use of AI in Market Research

Information Commissioner's Office (ICO):

GDPR / Data Protection Act 2018: https://ico.org.uk/for-organisations/guide-to-data-protection/

Legal bases for processing data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

ICO guidance on Big Data: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

ICO International data transfer agreement and guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/

Artificial intelligence: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/

2 Other useful references

ABPI:

ABPI Code of Practice for the Pharmaceutical Industry 2024: https://www.abpi.org.uk/reputation/abpi-2024-code-of-practice/

ABPI/BHBIA Guidance notes on collecting adverse events, product complaints and special reporting situations during market research

ABPI Guidance notes on the management of adverse events and product complaints from digital media

Artificial Intelligence:

Clinical Leader – overview of AI including definitions: '6 Ways AI is Transforming the Life Sciences (Already)'

MRS Guidance on Using AI Related Technologies – updated April 2025

MRS Clientside Best Practice Guidance – Client Perspective on inclusion and AI – updated July 2025

Copyright, database and electronic communications:

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011: https://www.legislation.gov.uk/uksi/2011/1208/made

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

The Copyright and Rights in Databases Regulations 1997: http://www.legislation.gov.uk/uksi/1997/3032/made

The Government Intellectual Property Office: www.gov.uk/government/organisations/intellectual-property-office

GDPR:

European Commission's data protection website: https://ec.europa.eu/info/law/law-topic/data-protection_en

Information on EC approved SCCs: https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_en

Information on EC BCRs: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

Information security:

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

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

Open Data:

Open Government Licence https://data.gov.uk/terms

NHS England https://digital.nhs.uk/data-and-information/data-tools-and-services/data-services/hospital-episode-statistics

British Healthcare Business Intelligence Association
Fountain Precinct, Balm Green, Sheffield, S1 2JA
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk

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