BHBIA Data Analytics
Considerations for CRM management

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

INTRODUCTION

This article suggests some of the things to consider when managing a customer relationship management (CRM) system, with specific regard to the data held and collected within the CRM. Although the article refers to CRM throughout, similar considerations should be given to separate account management systems, which often hold similar data.

Included in this document:

- Which data are appropriate for storage and collection?
- How should the data be stored?
- How can the data be shared?

As with most uses of secondary data, the key principles underpinning data protection law should guide the use and storage of data. The BHBIA's Ethics and Compliance Committee has published several articles on data protection requirements and their relevance to data analytics and secondary data, so these principles are not repeated here.

WHICH DATA ARE APPROPRIATE FOR STORAGE AND COLLECTION?

All users of the CRM should have training on the appropriate use of the systems and data within them before being provided with access, and a training record should be kept as evidence. This will help to ensure only appropriate data are captured. Organisational compliance aspects should form an early part of the training (e.g. what constitutes compliant practice for company x).

Personal Data

Any data held within the CRM on Healthcare Professionals (HCPs) should be relevant to the business interaction. For example, it may be relevant to hold a doctor's year of qualification and practice address, but holding their date of birth or home address is unlikely to be relevant to the business interaction. In general, hold the bare minimum required for the business practice and 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 through this means for marketing purposes. A lawful basis for the use of this data for any other purpose must be established e.g. consent or legitimate interests.

Home address and other personal data about representatives irrelevant to their job should not be stored within the CRM system. Their data is not public domain, data protection law requires that companies do not process personal data unnecessarily or unlawfully (i.e. without a lawful basis), this includes collecting and storing personal data.

The company must make sure that any personal data on HCPs held within the CRM is up-to-date and accurate. Purchasing a list from a specialist list provider can help to ensure data complies with the data protection requirements.

Free text

Free text fields within the CRM enable valuable information to be captured, but they should be used sparingly, with caution, and with 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 respond and resolve 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 HCP to see it if requested. Data Protection law

Individuals have the right to access all personal data related to them under data protection law. If such a request is received, it would normally be best practice to refer this to your legal department for guidance. See the BHBIA's Guidelines on Data Subject Rights available in the Secondary Data Guidelines series.

Following each interaction, notes should capture the contents of the discussion and objectives for a next visit if agreed with the customer. The representative should be happy to share these with the customer if requested to do so.

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 and no inference of bribery can be levelled at a later date.

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 Legal & Ethical Guidelines.

HOW SHOULD THE DATA BE STORED?

Consideration should be given to where the data are stored, as CRM's almost always contain personal data, which has to be protected under data protection law.

The 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 sufficient contractual arrangements will need to be put in place.

Field based devices enabling access to the CRM (laptops, tablets, smart phones) should be 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 stored securely. Systems should be designed and developed with privacy requirements built in.

HOW CAN THE DATA BE SHARED?

Where companies are using medical (non-promotional) representatives (sometimes called MSLs) and commercial salesforces, care should be taken to make sure that data entered into the CRM by the medical reps 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 a head office based outside of the European Union (EU), make sure that adequate contractual arrangements or binding corporate rules are in place to permit the transfer of personal date (under Data Protection law), alternatively supply anonymised or aggregated data only.

For further information see:

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

ABPI Code of Conduct
https://www.abpi.org.uk/our-ethics/abpi-code-of-practice/

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

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

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

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

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

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

Updated August 2020