BHBIA

BHBIA Ethics & Compliance

Online Security
Compliance: The New Normal

Introduction

The Covid pandemic has changed our attitudes and behaviours profoundly in the business intelligence (BI) world, and some of these changes are going to be long lasting. Understanding where the pandemic is leading us in terms of market research (MR) and data analytics (DA) practices and identifying the compliance implications is necessary so that we can alert and equip members to deal with these.

During the pandemic there has been a necessary shift away from face-to-face MR and whilst it will likely return post-pandemic, it is probable that a greater proportion of our work will remain online post pandemic, from research analytics and project management through to fieldwork. Therefore, a heightened sensitivity to online security will be one of our new 'norms'.

The BHBIA's Ethics & Compliance Committee is providing this guidance as general information for its members. There is no one-size-fits-all approach to the management of risk, and members are encouraged to consult with senior management, their IT department or outsourced vendor, or their organisation's information security policies when assessing how technology will fit into their working practices. Whilst every reasonable effort is made to make sure the information is accurate, no responsibility for its accuracy or for any consequences of relying on it is assumed by the BHBIA.

Compliance Issues

Remote workers, especially freelancers or small businesses, do not enjoy the same level of IT security infrastructure provided by large corporations or in the traditional bricks and mortar setting. Some common considerations and questions to ask ourselves include:

1. How do we handle data transfer and storage? The use of free document storage and sharing services in particular, e.g., BOX or Google Drive, can carry data protection risks:
    - Many free services use cloud-based technology with servers located abroad or in unknown locations.
    - Free or trial versions tend to offer limited control over security and retention of the stored data. Trial versions will also expire by virtue of their nature.
2. How do we maintain and demonstrate respondent and/or end client anonymity when video conferencing/webcam technology is used?
3. How do we make sure we capture signatures securely remotely?
4. How do we ensure confidentiality and security when conducting online MR? And consider the well-being of participants?
5. When we utilise self-recorded MR or ethnography (i.e., participants audio record and/or film themselves in their own environment), how do we ensure this is done in accordance

with the principle of data minimisation? We need to take into account the risk of other individuals being recorded without their consent (accidental intruders).

6. How do we ensure cross-platform compatibility when moving data around?

Practical Tips

We offer some practical tips for MR and DA practitioners.

- Manage access control. It is very important to decide who has access to what and for what function (read only, read/write or full admin). Best practice tells us that users should be granted access based on the **least privilege** and **need-to-know** principles. In other words, give users only as much access as they need to perform their role, and nothing more. In addition, access should be revoked at the earliest opportunity.
- It's essential for teams to be able to collaborate in shared folders or drives, but you should make sure you document how access is granted (and revoked) and who has access to assets. It's a good idea to review this at regular intervals to revoke access that is no longer needed.
- Ensure document signature capture software is secure (e.g. make sure the data will be encrypted, the signature itself will not be freely accessed by others without permission, that firewalls are in place as is multi factor authentication (MFA)).
- Carry out a Data Protection Impact Assessment (DPIA) and identify steps you can take to mitigate the risks when using a new platform, different methodology or assessing online security in general. You can find further information on DPIAs and the ICO's template **here.**
- Provide compliance reminders when using online platforms, e.g., reminding respondents how to log in, whether to use a pseudonym, their initials, or their full name depending on anonymisation/data protection requirements applicable to the activity and enforce the password update policy.
- When conducting online moderation the following steps should be considered: a) using headphones to minimise exposure to audio; b) using screen protectors to avoid anyone being inappropriately recorded or exposed to video feed.
- For self-recording or ethnography, remind participants that any recording, unless required for the study, should not include any other individuals but themselves. Provide:
  - Guidance on the positioning of the camera.
  - Advance warning to consider indoor (e.g., family members/people living in the same house) and outdoor (capturing passing members of the public) scenarios.
  - If there were accidental intruders in the footage provided, researchers are unlikely to have a legal basis to process this content and shall redact it from the files at the earliest opportunity, and at the very least before further processing or transfer to another party.
- Changing the display name on Zoom/Teams to protect identities and changing the background to eliminate unnecessary exposure of personal artefacts.
- Have processes in place to review any self-recorded data to remove/anonymise any personal data from other individuals (unless required for the MR).

- Provide guidance specific to remote interviewing, e.g.:
  - Do not state your true/full name – for participants
  - Do not have anything else open on your computer when screen sharing – for researchers

Final Words

Technology always moves faster than legislation but the principle of lawfulness, fairness and transparency still applies to our practice. Clear, simple and consistent instructions will always help in terms of data protection, security and adherence. Regular reviews especially if timed to coincide with major technology upgrades will add value.

Further Information

IT Security top tips (computer security, email security, fax/paper security and staff training)- https://ico.org.uk/for-organisations/guide-to-data-protection-1998/it-security-top-tips/

A practical guide to IT security (ideal for small business) - https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

Online safety - https://ico.org.uk/your-data-matters/online/social-networking/

It is not the intention of the BHBIA's Ethics & Compliance Committee to recommend, endorse or otherwise approve a particular solution, platform, or technology over another. Any reference made to a commercial product is for illustration purposes only, and members are encouraged to review the range of solutions available on the marketplace to find the one that will be right for their organisation.

Prepared by the BHBIA's Ethics & Compliance Committee March 2021

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