DATA PROTECTION & SECURITY POLICY

July, 2021

HANOVIA LIMITED

Address: No. 8, Ahmed Musa Crescent,
Jabi – Abuja
Website: www.hanovialimited.com
Email: info@hanovialimited.com

Table of Contents

1. BACKGROUND

1.1 Data Management

At Hanovia Limited, we work with the state-of-the-art data collection tools to ensure high quality data is delivered to our clients. The firm has conducted and managed over 100 surveys between 2012 and 2022 electronically. These surveys were conducted with tablets running on *CSPro*, *ODK*, *SurveyCTO* (using CATI and CAPI approach) *SurveySolutions and Kobo toolbox* data collection platforms. The firm has setup adequate data protection and security protocols which are deployed for the various quantitative and qualitative surveys conducted. Also, having worked on several surveys, we have developed a robust protocol to enhance data quality. The protocol is highlighted below:

a. Programming and deploying of questionnaires to the required data collection server for each survey. The *SurveyCTO* data collection platform is used for most of our surveys using the computer-assisted personal interview (CAPI) technique.
b. Data collected is transmitted from the tablets to a secured remote *SurveyCTO* server on daily basis for proper data management.
c. Timely high frequency data quality checks and other coherent checks are conducted on the data uploaded to the server using the data cleaning and quality assurance checklist. Some of the proposed areas considered during the data quality checks are: completeness checks, coherence checks, constraint checks, skip pattern checks, duplicates observations, labelling of variables, and recoding of other specify response and early identification of any inconsistencies in data gathering before the data collection is completed.
d. Submission of raw and cleaned datasets for quantitative research and audio files and quality assured transcripts for qualitative research. The quantitative datasets are converted into *Stata,* SPSS and MS Excel or any other format as may be required by the Clients.

2. DATA PROTECTION AND SECURITY

Sensitive data are vulnerable to inadvertent disclosure and targeted attacks. If data security protocols are not adhered to, data may be disclosed through e-mail, device loss, file-sharing software such as Google Drive, Box or Dropbox, or improper erasure of files from hardware that has been recycled, donated or disposed of.

2.1 Data protection and security procedures

Hanovia's data protection and security procedures are highlighted below:

a. All hardware that come into contact with study data should remain protected including: laptops, desktops, external hard drives, USB flash drives, mobile phones, and tablets. Theft or a cyber-attack may target either personal data of respondents or data belonging to the firm.
b. Separate Personally Identifiable Information (PII) from all other data as soon as possible. Data pose the most risk when sensitive or confidential information is linked directly to identifiable individuals. Once separated, the "identifiers" data set and the "analysis" data set should be stored separately, analysed separately, and transmitted separately.
c. All personal data collected and processed by the firm is only accessible to data managers and head of data management department
d. Staff are required to keep computer passwords confidential and are not permitted to leave manual records containing personal information where they can be accessed by un-authorized individuals
e. At the end of every survey, all data with PIIs shall be extracted from staff's laptop to a secured cloud folder and dedicated and password protected external disk for contingency. This is to avoid movement of computers with data in them
f. Individual members of staff required to handle sensitive data in the course of a project or survey in the organization signs a confidentiality agreement which will explicitly state that unauthorised disclosure or a breach of the Data Protection and Data Security Policy may result in disciplinary action.
g. Access to sensitive personal data and personal data of respondents is strictly controlled and held in a secure drive to which access is restricted. Similar arrangements are in place for client's personal data where it is stored with encrypted devices.
h. All staff with access to personal data ensure that when work documents are unattended to, no personal data or sensitive information, is left unsecured.
i. Portable external hard drives as the organization electronic systems are available to staff with appropriate levels of remote access.
j. Staff are not permitted to use USBs for the storage or transfer of personal data or sensitive category data

k. Similarly, portable hard drives that aren't password protected are not used as a means to transfer personal or sensitive data unless suitably encrypted. In areas where such devices are used for archival purposes, they should be stored securely and allocated in the right directory of documents.

- In all cases, any encrypted USBs and portable hard drives given to staff for handling data during a project must be returned on request. When in use, they are kept securely, and appropriate encryption should be in place to ensure their location is known at all times.

2.2 Transcription

Hanovia's policy on transcription is detailed below:

a. If an individual professional transcriber is to be used, he or she must sign a non-disclosure agreement form
b. Files are always encrypted and password protected before transferring to the computer of the transcriber. All audio files are transferred to the transcriber's computer via secured cloud folder
c. Once the recordings have been transcribed they are saved by the transcriber as password-protected word documents and transferred to the secured cloud folder. The password shall be sent separately or provided by telephone
d. Transcribers are required to securely deletee all data from their computer. To further confirm deletion, transcribers will be asked to share a screenshot of the folder containing all transcripts and audio files on their laptop. This is to ensure all project-related documents and audio files have been properly deleted as agreed.

3. DATA STORAGE AND ACCESS

This policy describes the requirements for storing qualitative and quantitative research data. These requirements include data storage platforms based on the sensitivity of the data, the ability to execute reliable data backup and recovery procedures, and manageability and configurability of data access control.

Among various storage mechanisms for data storage, the firm considers the sensitivity of the data and acceptable standard stated in the IBR for data storage and accessibility for the clients. The data management team ensures that all stored data are encrypted at many levels and at multiple stages of the data lifecycle.

Hanovia's encryption method involves the conversion of data to code that requires a password or pair of "keys" to decode, and this is the standard practice for all surveys executed by the firm. In order for the client to gain access to the encrypted data, the data manager shares the code and password in a different mail thread.

All survey data are stored and made available to the client through the encryption and cloud storage described below:

- **Device-Level Encryption:** The data manager ensures that all devices including computer, tablets, mobile phones, and any other hardware for data storage and/or primary data collection are password-protected and encrypted. This method protects all files on the device, and requires a password upon device start-up. Furthermore, all tablets have *AppLock* installed to prevent users from accessing other applications during data collection. This protects data from being transferred across applications in the course of data collection.
- **Server-Level Encryption:** Data from the field are uploaded to a designated web secure server (e.g. *SurveyCTO, KoboCollect,* etc.). All data on the server are encrypted and only accessible with the encryption key.
- **Cloud Storage:** Raw datasets and other data related documents are uploaded to a secure designated cloud folder.

4. DATA TRANSMISSION

Data that are encrypted are stored on a disk encrypted drive, or on a secure server.

In Hanovia we have employed adequate and reliable safe transmission methods which include

- The use of survey software with encryption features, such as SurveyCTO to supports encryption during data collection and transmission to a central server
- Uploading all encrypted data related files to Dropbox via Boxcryptor

The firm in agreement with clients usually develop standard operating procedures for checking and responding to breaches in data collection and transmission following the agreed upon method for sharing data.

4.1 Data Collection Device Security

We have deployed simple steps that data managers and field personnel can take to ensure their devices remain secure. These steps include:

- Create and use a password-locked screensaver and timeout lock for tablets and devices for data collection
- Dfferent passwords are used for different project to avoid weak points for accessibility and data fraud
- The IDs and PIIs from the datasets are backed up regularly in at least two separate locations
- computers and platforms used regularly for data cleaning are checked regularly for new versions of software. New versions of these software and platforms are updated to fix security problems

Data can also be transmitted on the client's preferred platform based on their data transmission preference and protection policy. We are familiar with the use of *Moveit*, *KiteWork*, *OneDrive* etc. for data transmission.

5. DATA DESTRUCTION

In Hanovia, all survey data and data related documents are stored in a dedicated external hard disk for contingency and destroyed after 12 months upon signed approval from the client. However, depending on the clients' policy, data destruction may be done before 12 months or after 12 months. Our data destruction policy includes the following:

- Deleting all data related files from the storage devices
- Erasing all electronic files or media containing personal data so that the information cannot be read
- Shredding data related papers
- Survey data are only maintained for as long as the client desire or stated in the IRB.
- The Data Protection Officer (DPO) in Hanovia frequently audits the firm's data holdings monthly and keep track of what data is destroyed when and how;