Digital Information Storage and Security Policy and Procedures

HiFlex Physio

Policy

This policy applies to all HiFlex Physio employees.

HiFlex Physio is committed to providing valuable and accurate evidence of business decisions, activities, research, and transactions. In doing so, the responsibility to create, store, and maintain accurate and reliable information is vested upon the organisation.

In addition, HiFlex Physio is committed to the principles and practices retained in the Information Management Standard of the National Archive of Australia.

In our commitment to keep all business activity transparent and honest, we retain the access of all business information to employees except under the following circumstances:

- Client information, the access to which is limited to the direct personnel handling the client
- Member information, the access of which is limited to Customer Service s and the Management.
- Sensitive financial information, the access of which is limited to the finance department and the individuals directly involved in the transactions.

The purpose of this policy is to ensure that all information practices related to the creation, storage, security and maintenance are being carried out efficiently and truthfully.

Procedures

Maintenance of Digital Information

Business information must be created and maintained by providing reliable and accurate accounts of business decision and actions. This must include all pertinent information to support business needs, which included names, dates, timeand other key information.

Storing digital information must follow the steps outlined below:

1. Once business information is created, it must be saved into a corresponding folder related to its purpose and designation.

2. All filenames follow the following format: [Date Saved (DD-MM-YYYY)]-[Document Title]

3. Files must be saved under corresponding to the project and/or business function the information supports. For example, Information regarding business operation must be saved under the folder “Business Operations.”

4. Sub-folders may be made in accordance with need for organisation and efficiency.

For example, an interview transcript for current market research may be saved under “Transcript” subfolder saved within the “Marketing Research 20XX” folder.

5. All relevant personnel must be notified of recorded information in the database.

Security of Digital Information

Business information must be maintained using proper security procedures to ensure that all necessary steps are taken to protect digital information from the likes of information theft, spyware, phishing and viruses.

1. All information must be saved in the cloud database created by the organisation.

2. Access to the following types of information must be limited to either the direct supervisor or relevant stakeholders:

- Research information
- Market research

3. For very sensitive information, the information must be saved with a password. Sensitive information corresponds to the following:

- Financial records
- Employee records