Data Backup and Storage Policy
Section: Data Management

Prepared by:	Barend Botha, Kieara Smit, Charl Bezuidenhout
Approved by:	C.I. Bezuidenhout
Revision date:	1 July 2020
Effective date:	1 July 2020

Statement of Policy and Procedures relating to 'Heardat Access and Security"			
Manual	Information Technology	**SPP No**	HDDBS 2.1
Section	Data Management	**Issued**	1 July 2020
Subject	Data Backup and Storage Policy	**Effective**	July 2020
Issue to	Employees, clients & users, external contractors	**Pages**	1-3
Issued by	Charl Bezuidenhout	**Replaces**	HDDBS 2.0 (May 2020)

1. Policy Statement

Data must be backed up and stored locally in a protected location on a regular basis.

1.1 Every day at 00:00 data must be backed up on the two separate, alone standing and nonaffiliated servers where data is kept.

1.2 Included in the storage and backup protocol, data is also backed up on to two separate external hard drives which is permanently locked up and stored on different sites. Most importantly, all backups of data herein using any method must ensure that all and any data is encrypted.

2. Purpose

2.1 The purpose of this policy is to specify the procedures for storage, backing up data and facilitating the recovery of important data in the event of accidental or intentional corruption, loss or destruction.

2.2 For data critical to the ongoing operation of the business, backup data kept at an offsite storage location will facilitate keeping the business operational in the event of a physical disaster at the original site. Furthermore, data is securely encrypted and stored on additional certified servers.

3. Scope

This policy applies to all employees, directors, clients and affiliated parties of Heardat who create, capture, process, import or have access to any data of any client, third party or clients or patients of the clientele of Heardat. Regardless of the ownership of any data.

4. Responsibility

4.1 All departments are responsible for identifying ownership for their data that requires backup. For all data that qualifies, the owning department must ensure that procedures are in place to back up their data whenever it is updated and to store the backup copies as required.

4.2 *Mr B. Botha*, herein representing Midnight Code Development ensures backup are effectively executed and stored according to policy on a daily basis.

4.3 The client is solely responsible for obtaining consent from their patients/customers for the electronic storage and processing of their personal and medical information by using a third party as per the Personal of Personal Information Act of South Africa. The third party herein refers to Heardat (Pty) Ltd.

4.4 Heardat shall not engage in any data processing or storage without the consent AND formal instruction from the client/health practitioner.

5. Definitions

5.1 **"Critical data"** is that data which is needed to continue the operation of a business.

5.2 **"Data backup"** means making a copy of data such that the copy may be used easily to recreate the original data organized in its original format.

5.3 **"Data medium"** means a physical object on which data may be stored (e.g., magnetic tape, tape cartridge, optical disk [CD-ROM, DVD], disk cartridge [ZIP, IOMEGA, 3M SuperDisk], or removable hard drive). Other historical data media not typically used today include punch cards and paper tape.

5.4 **"Offsite"** means a physical location other than where data is being processed. Its location must be far enough removed so that data stored offsite is not subject to the same physical risk from foreseen disasters. Note that if the objective is to protect against data loss in the event of a building fire or other disaster that restricts access to the building, a location in the same or adjacent building is not suitable as an offsite storage location.

5.5 **"Client"** means the person or entity that is legally binded as the customer to Heardat

5.6 **"Health practioner"** refers to client but in the personal form such as the responsible medical practioner.

5.7 **"Patient"** refers to the patient/client/customer of the client.

5.8 **"Third party"** refers to the relationship between the client's patient and Heardat, and vice versa.

6. Procedures

6.1 The backup copies must be on a storage device physically separate from the original. For example, if the data to be backed up is on a hard drive, the backup copy must be on a different hard drive and on the minimum of 2 cloud servers not affiliated with each other.

6.2 The backup data must be on a medium and in a format that can be easily used to recreate the data that has been damaged; however, it need not be identical to the original medium provided that the data may be restored to the original medium. For example, if the original data is on a hard drive, the backup may be on a removable disk, tape or optical medium from which the data may be copied back to a replacement hard drive in its original format. If the original data is organized in a

specific database type, the copy must have enough information to recreate the database. However, the main source of data storage and backup remains within the cloud servers.

6.3 For offsite backups, the following must be maintained:

6.3.1 List of offsite locations where backup data may be easily located and retrieved.

6.3.2 List of procedures that create backup data and cause it to be shipped and stored at the backup site. In the case of more than one offsite location, each entry in the list also includes a reference to the corresponding offsite backup location.

6.3.3 All data of the Heardat Client remains the clients property. Heardat act as a tool to process data in the desired way. Refer to 4.3 and 4.4

6.3.4 No data may be altered or changed, added or deleted with out written concent from the client.

7. Property and Ownership

7.1 Any data captured, processed or inputted by the client and/or Heardat personnel that is owned by the client such as patient information will always remain the property of the client and should, and will always be made available by Heardat to the client post formal request.

7.2 Heardat will back up all data as set out in Section 6. When the Client cancels their subscription with Heardat, all data captured and stored by the client or provided to Heardat in any form shall be kept for a maximum of 30 days. Thereafter all data of the client will be permanently deleted for the protection of Heardat, the client and the client's customers.

7.3 Point 7.2 subjects to the account status of the client. Should the client's account be in arrears, Heardat will withhold all and any data untill the client's account is settled. Subject to the conditions of 7.2.

7.4 Should the client at any time request manual data extraction once off or on a regular basis, the client will be quoted and charged an administration fee. Depending on the extensiveness of the data, the client maybe charged between R0.20 to R1.50 per patient export and inculdes all data provided or captured either by the client or on the clients behalf.

8. Attachments

None

The End