DataHEALTH Customer Responsibilities

Thank you for choosing DataHEALTH as your HIPAA compliant cloud backup and storage provider. We strive to provide excellent customer service and technical support. To ensure the highest rate of successful backups, please review the following Customer Responsibilities and keep them for reference. You may reach us at Support@DataHEALTH.com or 888.656.3282, option 2.

1. **Review your backup logs, at least twice a week.** Review them even if you've selected email alert options. Make sure backups are processing routinely, without error and the selected files and folders are backing up. A successful connection can occur and backup 0 files if your file path changes or someone deselects the files. When looking at the logs, pay attention to the number of files that have backed up. Also, emails get redirected by email routers all the time to the trash or junk bin. Don't solely rely on email alerts. Your backups are crucial in the event of a server crash, make it a habit to review the logs on a regular basis. If you need instruction, please contact DataHEALTH.

2. **Watch for an unusual or unexpected increase in the amount of files being backed up.** This could be an indication of a virus or malware infection in your files. Immediately contact DataHEALTH in this instance.

3. **Promptly respond to all forms of communication from DataHEALTH.** i.e. failed backup alert, past due account notices. Inform office staff to promptly pass along messages from DataHEALTH.

4. If you acquire a **new server, change hosted providers, have the server rebuilt or perform hardware maintenance** on the server, the **DataHEALTH backup software MUST be re-installed.** Call DataHEALTH ASAP.

5. **Changes to your network configuration or backup file path/location** (by you or your hosted provider) could mean your backup selection needs to be changed. Call DataHEALTH for assistance.

6. If you or your hosted provider performs **upgrades to your EHR or database**, contact DataHEALTH for assistance in selecting database for backup. **If it is not selected, it will not backup.**

7. **New or changed software and files will NOT be added to the backup automatically.** If you want them backed up, call DataHEALTH to have them added. (i.e., upgrading Quickbooks) (Review selections routinely.) **Again, if it is not selected, it will not backup.**

8. **Keep adequate, active and updated virus protection and malware protection software.** This is the first line of defense for your network. The moment you think you may have a virus, call DataHEALTH immediately to secure the most recent backup. Server (hosted or local) and all peripheral machines should be protected.

9. **Billing questions must be reported within 45 days** of receiving your DataHEALTH invoice. No refunds or credits will be issued for invoices older than 45 days.

10. **When you change your administrator password, call DataHEALTH.** Changing your administrator password will stop your account from backing up.

11. **Report any contact information change, ASAP.** (I.e. phone number, address, email address, authorized users, IT consultant, change in ownership or business structure, or cancelation of account) Call or email DataHEALTH or log into the customer portal at: myportal.datahealth.com to update your account.

12. For a **data restore**, we prefer you call **DataHEALTH for assistance**. An authorized account user needs to call for the restore. Data should always be restored to a temporary folder on a different drive from your production data. Always verify the accuracy of restored data before overwriting your production data.

13. Account **will not be cancelled** if you don't notify DataHEALTH in writing. Email support@datahealth.com or fax to: 270-423-0000. If your account stops backing up, you will still be billed for the data already stored.

Revised 7/2022