

Guidelines for System Administrators

for all IHS Software

Administrative Privileges

For full functionality of the software, even standard users will need to have full read and write privileges to specific folders, even if they are not administrative users on that computer.

The IHS software uses, by default, the following hard drive locations; to store patient data, system settings, and export data:

- **C:\IHSProgs:** This location stores the programs and settings. Older versions of the software also included the patient data in this folder. The location may be modified at the time of installation. The installation path must not contain spaces. All users must have full rights to this folder.
- **C:\IHSDData:** This location stores the patient data including demographic information, patient list, system log, and schedule. The path may be modified from the Patient List window to point to a different location. All users must have full rights to this folder.
- **C:\IHSEXPData:** This location is intended for exporting patient data. A different export path may be selected from the Data Backup Utility. Full rights to this folder is not required, unless workflow requires data export.

In addition, there must not be restrictions in place for users to access USB devices, as they would prevent proper operation. Installing the hardware driver using the included installation utilities (IHSDriverInstallation32.exe or IHSDriverInstallation64.exe, depending on the OS bits) is highly recommended to allow for standard users to change USB ports without the need of an IS technician. Alternatively, plug the device into all possible USB ports during setup, and ensure the device is detected properly, so that users are not impacted by a change of port. If you prefer to install the device manually, all device drivers can be found in the main software installation folder (typically C:\IHSProgs).

Patient Data Location

As mentioned in the previous section, the default location for patient files is C:\IHSDData. The location of the data can be changed; however, there are a couple of requirements to keep in mind:

- The data path must not contain spaces. Folder names containing letters, numbers, underscores, and dashes are valid.
- The data path should never be a root folder. Root folders have limitations as to the number of sub folders that can be inside them; if the patient database grows past this limitation, data might become inaccessible. Sub-folders are not affected by this limitation, although access might become slow when there are too many folders inside them.

There are two ways to modify the standard data path. Doing it through the IHS Launch Pad program is the recommended procedure:

1. From the LaunchPad program click on **[PATIENT > OPEN]**.
2. In the Patient List window, click on the **[CHANGE DIR]** button.
3. From the menu that opens, select **[OTHER]**.
4. Change the Drive selector if saving to a location other than C, or to a mapped network drive.
5. Browse the folders to find the new destination, double click on the folder so it shows an open folder icon and its contents, then click the **[OK]** button.
6. Click the **[REFRESH]** button at the top right to check if there are patient files already in that folder. Consult the LaunchPad manual for instructions on how to backup the patient data to this location first, if needed.
7. If there are already patients listed, open one, if not create one by clicking the **[New]** button. This can be a made up patient for setup purposes only.
8. Open each of the individual IHS programs by clicking on their respective icons in the LaunchPad, then close them. This will make the new data location propagate.
9. Finally exit the LaunchPad.



For additional help:
e-mail: support@ihsys.com
phone: (800) IHSYSTEMS (USA)

SNGEN020 - EN - 201202

The next time the programs are launched, the data path should be the new one for all programs. The current data location is listed in the upper mid section of the LaunchPad window, right above the IHS logo.

This procedure can also be completed manually by editing the individual settings files for each program. This process is not the recommended method, because it requires manual editing.

1. Make sure all IHS programs are closed. If they are not all closed, any changes will be reverted when you close them.
2. Browse the installation folder C:\IHSPrgs\Settings_IHSPrg to find the file called IHSPrg.INI.
3. Open the file in Notepad and modify the DataDir variable to the correct location.
4. Do the same for other programs by finding their corresponding INI files in their respective Settings folders.

Be careful when editing these files. Do not change any other lines and be careful to maintain the internal structure. If you make a mistake and can't seem to be able to fix it, simply delete the INI file; then open and close the program in question, the programs will re-create them automatically.

In some instances it may be advisable to create a symbolic link to the C:\IHSDData folder. This will allow the use of any folder as the data storage

Identifying Patient Information

Information identifying the patient could be found in the following locations:

- **The Patient List:** the IHSDMGLIST.DAT file, found in the patient data directory. This file contains a list of all patients including their name, system identifier and secondary ID. This file is encrypted. Older versions of the software will have an unencrypted file named DMGLIST.DAT instead.
- **Patient Demographics Files:** the individual files with extension ".IHSDMG" can be found inside each patient folder. These files contain the patient demographic information. These files are encrypted. Older versions of the software will have unencrypted files with the ".DMG" extension instead.
- **User Notes:** user generated text (TXT) files, in the individual patient folders, may contain patient demographic information or diagnosis, if entered by the users. Users should be mindful of the information entered in these fields as the information in these notes is not encrypted.

- **PDF reports:** usually located in the patient folder, include the patient's name and identifier in the contents of the file. As a matter of cybersecurity, these files should be password protected by the users.

Note that exported data may have identifying information removed by checking the appropriate box in the Data Backup Utility. This should be done every time the data is exported for the purposes of sending it to external locations.

Encryption

Encryption can be used to address some privacy requirements in your institution or region. In general, standard encryption algorithms do not affect the functionality of the Intelligent Hearing Systems software or hardware. Encryption software programs such as Microsoft Windows BitLocker are perfectly suited for the task without negative effects on functionality. Built-in hardware encryption solutions do not affect the use of IHS programs either.

More comprehensive methods of encryption, such as Symantec Endpoint Encryption Device Control may affect functionality. Programs such as the one mentioned, encrypt all information being transmitted to externally connected devices. This can cause the instruction sets sent by the IHS software to be unreadable by the hardware; preventing data acquisition.

For proper operation with the more comprehensive solutions, the IHS device must be white-listed so that the sending of instruction sets is unhindered. Consult the documentation of your encryption software for instructions on how to achieve this. Since no patient information is ever sent to the IHS hardware, this exception will not affect privacy.

Antivirus Software

There are no known incompatibilities with IHS hardware or software to operate in a computer with Antivirus Software installed. The IHS software has been tested, and found to be fully operational, in computers using antivirus software from Symantec, Trend Micro, McAfee, AVG, and Microsoft.

If at any point your antivirus program reports a file inside the installation folder to be infected, please contact IHS to confirm the validity of the file and/or obtain a replacement. You may also create a scanning exception for the IHS software installation folder and the patient data folder mentioned in previous topics. Consult the documentation from the Antivirus software manufacturer for instructions on how to create exceptions to a file or folder.