# Senscio Systems System Approach to assure PHI is protected

# Data Security of Protected Health Information (PHI)

Technical Security

Senscio Systems has designed the lbis Software system with PHI security in mind. The lbis system employs the following methods to secure PHI.

1. All identification information (name, address, date of birth, phone numbers, gender) are kept separate from health information. An ID is assigned to each person. The identification information and associated ID is saved in an encrypted database.
2. Health data is saved in a separate proprietary data repository. The health data cannot be read without our proprietary code. No identifiable information is saved in the health data repository. The ID is used to link the health data with an individual only when the health data is displayed.
3. All health data is transmitted back and forth from the repository, encrypted.
4. A separate encrypted database is used to store health notes, written by clinicians and caregivers, since they may contain identifiable information.
5. Access to health data is gained through applications that require a login with a password. Clinicians have access to patient’s health data. Caregivers who are approved by the patient also are granted access to patient’s health data.
6. All data is stored in a dedicated hardware with a physical firewall that separates it from other hardware. The physical firewall can be monitored for data access.

Limited Access

Senscio Systems will limit access to health data to only those personnel who are supporting the lbis deployment. Access will be granted in order to troubleshoot technical problems, customize the lbis service, perform analysis and prepare reports. Printed copies of documents containing PHI will be kept secured until destroyed.