Identity Security and the COLLAGE National Data Repository: What Members Should Know

In COLLAGE iForms (the assessment software application), National Numeric Identifiers (NNI) include Social Security Number, Medicare Number and Medicaid Number. NNI have recently assumed great importance relative to identity theft and are regarded far more protectively than previously may have been the case. Experience shows that the resident populations of most COLLAGE member sites, and therefore the staff as well, are particularly sensitive about this issue. Despite the fact that Business Associate Agreements between the members, the joint venture parties and the software developers cover the HIPAA PHI privacy and security issues, COLLAGE is taking exceptional care to prevent the unnecessary or inadvertent exposure of NNI stored in the National Repository.

All face sheet and assessment data transmitted to the repository is encrypted before it leaves an organization, and everything is unencrypted EXCEPT NNI once it reaches the repository. NNI CANNOT BE DECRYPTED without the organization's unique electronic key that is always in the possession of the COLLAGE member. This incidentally provides members with a secure, back-up system for storing their data. If a member organization authorizes the use of NNI, they will transmit the encryption key to the Repository at Hebrew SeniorLife (HSL) before any NNI can be read. Once a key has been transmitted, the iFormsReader application, held at HSL, can decrypt and access NNI. This might be done to allow for correlation of data in the COLLAGE Repository with other data held by CMS or other agencies that use NNI as record identifiers. A member also has the option of choosing not to have NNI transmitted with assessments at all. In this case, they can configure the iFormsUpload, application that transmits the data, to retain NNI and to only send the other face sheet and assessment information. Members retain the capability to transmit NNI at a later time of their choosing.
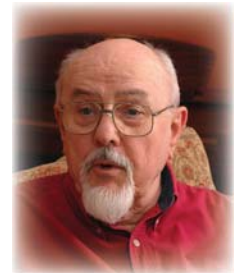
The basic process of transmitting, storing and accessing NNI and other data to the Repository is as follows:

1) iFormsUpload, the application that transmits data from the member site, starts automatically, usually during off hours at night. It is usually run from the file server which hosts the COLLAGE databases.

2) A connection is established over the Internet with the Repository in Boston, MA.

3) iFormsUpload sends login information and a Secure Sockets Layer (SSL) connection is established with the Repository.

4) As assessment records are identified as needing to be transmitted to the Repository, NNI (if sent) are encrypted using a symmetrical encryption algorithm with an encryption key retained by the iFormsUpload application.

5) Using the SSL connection previously established, everything is encrypted before it leaves the member site and is transmitted over the Internet. All data but NNI (if sent) is unencrypted for storage once it reaches the Repository.

6) When sent, NNI is stored in a table separate from any other data. It remains encrypted in storage as it was upon leaving the member site using the symmetrical encryption algorithm system. The client ID is stored with the NNI so it can be later connected to other records for that person should it be so authorized by the COLLAGE member.

7) At the discretion of the COLLAGE member, iFormsUpload can:

   a. transmit the encryption key for NNI along with the assessment records themselves,

   b. delete the encryption key previously transmitted,

   c. regenerate the encryption key used by iFormsUpload, or

   d. not send NNI at all.

8) Encryption keys that have been released by COLLAGE members are stored in their own table in the Repository and are themselves encrypted with another secret key known only to certain COLLAGE applications.

9) A separate application, iFormsReader, can decrypt transmitted encryption keys and use them to read NNI, correlate it to assessment data, and export the result to a private location as either a delimited text file or an Excel spreadsheet.

Further, at no time is NNI stored in the Repository in unencrypted form. If a member decides their NNI should be private again, iFormsUpload can re-encrypt the NNI previously transmitted to the Repository with a new key which is different than the one previously sent to the Repository and which is again held only at the Member site.