Synergistic Office Solutions
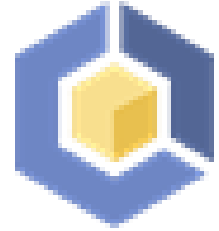
Topic: **SOS and HIPAA Compliance**
Document ID: **#116**
Product: **All SOS Products**
Revision Date: **July 27, 2020**
Author: **Seth Krieger**

HIPAA Compliance

While HIPAA rules and regulations are relevant to certain software products that you use, compliance requires more than simply obtaining software updates. The most significant aspects of this legislation mandate greater care and better procedures for the handling of all protected medical information, whether in electronic or paper form. It governs patients' rights to certain records, your response to requests for records, how you store and protect records, and much more that will surely require that you review and modify your current office procedures.

SOS has been engaged in an ongoing effort to provide its users with software tools that will allow maximum flexibility with regard to HIPAA compliance, but you must review your use of other software that you use for the production or transmission of medical data. For example, many providers probably employ a word processor to generate reports or other clinical record material. Compliance with HIPAA will require that you encrypt or otherwise protect such documents (including all existing documents) to prevent access by an unauthorized party who has, or could have, access to your computer system. It is essential that all providers take steps to educate themselves concerning the HIPAA privacy and security regulations. You can start with research on the internet (see, for example, http://www.hipaa.org/) but such research should be reinforced by participation in appropriate professional education offerings that are aimed at your specific type and size practice or organization.

HIPAA regulations impact existing SOS products in two areas:

1. Electronic data interchange (EDI) transaction sets (electronic claim filing).
2. Certain privacy/data security requirements.

**IMPORTANT:** *No software product will make your organization HIPAA compliant!* **Compliance is primarily a matter of office policies and procedures, most of which are <u>not</u> technology-based. SOS and other companies can provide you with some tools to assist you to achieve compliance, but it is up to you to configure and use those tools in a fashion appropriate to your organization's structure, size, and needs.**

Transaction Sets

The HIPAA transaction set standards affect all those who are submitting claims electronically, even those submitting through a clearinghouse or service bureau. SOS provides electronic claims submission modules to conform with the HIPAA-endorsed specifications for the submission of claims data. In addition, the HIPAA standards allow us to offer a module to automatically post insurance payments and adjustments by processing information contained in standardized *electronic remittance advice* files.

At the present time, SOS does **not** have any plans to implement the eligibility request (ANSI 270), claim status request (ANSI 276), or referral authorization (ANSI 278) transactions. In summary, then, with regard to the relevant, accepted, HIPAA standard transactions:

Transaction Standard	Status	Expected Release Date
ANSI 837: Professional and Institutional Claims	Coding complete.	Released
ANSI 835: Remittance	Coding complete.	Released
ANSI 270: Eligibility	No current plans to implement	n/a
ANSI 276: Claim Status	No current plans to implement	n/a
ANSI 278: Referral Authorization	No current plans to implement	n/a
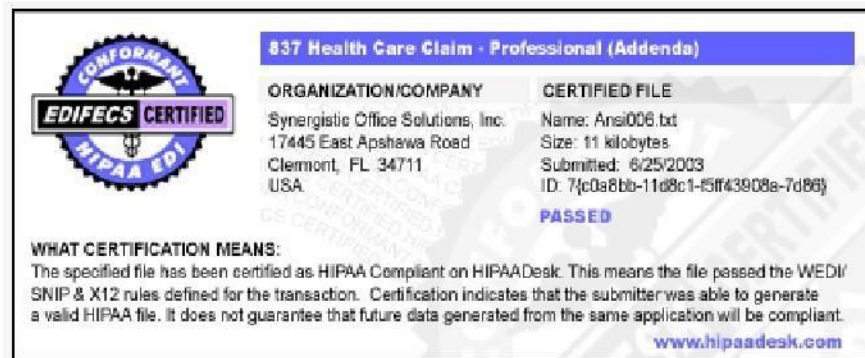
Code Sets

Some providers have also inquired about HIPAA-specified code sets. Both diagnostic (ICD) and service (CPT) code sets are available for your use within SOS Office Manager. Mental Health providers who are accustomed to using DSM diagnostic codes on insurance claims should note that these codes are not compliant except where they coincide with an existing ICD-9-CM diagnostic code. HIPAA standards require that ICD diagnosis codes be used on claims! As of October, 2013, SOS has provided a utility to assist in the transition from ICD-9 to ICD-10 diagnosis codes. The new codes are required starting in October, 2014 and will be fully supported in SOS products by June, 2014.

Privacy and Security

Although the spirit of the HIPAA privacy protections for health information requires changes in both procedures for handling health information (staff and management issues) and technical safeguards for information stored or transmitted electronically, the implementation of these protections has been broken out into a set of *Privacy Rules* (enforced beginning in April, 2003) and a separate set of *Security Rules* (enforced beginning in April, 2005).

To meet the Privacy requirements, it is essential to obtain training for all staff, create required documents (such as your Privacy Policy and Procedures manual and Notice of Privacy Practices) and begin logging information releases and other HIPAA-related activity. Among other things that you do to prevent unauthorized persons from having access to protected health information, you should implement real password protection in your SOS applications. You should change the

supervisor password from the default password, and you should require that all users select and use a *secure* password to gain access to the software. Passwords that are common knowledge within an office are not secure, nor are passwords written on scraps of paper taped to the monitor. In addition, you should review which user configurations include the option that permits them to access the database from other programs and disable this option for all users except those who should the right to access everything in the database.

SOS Security Enhancements

HIPAA has a general requirement that those working in a healthcare setting should have access to only the patient information necessary to do their jobs. Some have interpreted this standard to mean that users must use secure personal identifiers (such as ID codes and passwords) to access software containing protected information and that the software should provide for display or suppression of data based on the person's role in the organization. SOS implemented a full range of optional security enhancements beginning with the 2004 releases of its product line. Among these enhancements are the following:

Role-Based Security: SOS software includes an advanced security system that permits data to be hidden on a field-by-field basis, depending on the access right assigned to the user. SOS's role-based system allows each user to be assigned to one or more groups, such as "Appt Desk", "Provider", "Supervisor", and so on. You can then hide or disable selected menu items, windows, tabs, fields, and other controls to prevent each group of users from accessing or viewing anything that is not necessary for their job function. The same type of role-based security is extended to report generation. Unless a user belongs to a group that has been granted access to a particular report, the user will be unable to run it.

User Activity Log: If desired, SOS users may enable an option to keep a running record of who viewed which windows, for which patients, when, and whether information was added, viewed or changed. Companion reports permit monitoring of activity by user or by patient. In addition, archiving and careful storage of the database transaction log (SOSDATA.LOG) file of the database allows later determination of specific changes made to protected information, at specific times, by specific users, if this should ever be required.

Data Deletion Log: The system maintains a running record of any deletions of protected health information. This log contains the identity of the user, the date, the time, the nature of the data, and the patient with whom the information was associated.

User Login Tracking: The system records logins and program exits (ID, time, date), as well as password failures. There is an option to lock out user ID's after three unsuccessful password attempts.

Patient Visibility and Access Based on User ID: An option ties access to each patient's data to the ID used when starting the SOS application. Unless an ID is specifically cleared for a particular patient, that patient will not appear in patient selection lists and reports generated by that user.

New User Password Options: Other options require change of passwords at a user-defined interval, forcing use of strong passwords that contain numbers or punctuation as well as letters and/or a minimum length for passwords.