DocuTrac, Inc.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was the result of efforts to reform healthcare. The goals of this legislation are to streamline industry inefficiencies by establishing standards for health information, reduce paperwork, guarantee security and privacy of health information, reduce fraud and abuse, and assure health insurance portability for individuals with pre-existing medical conditions.

How does HIPAA Impact on Practice Management and Documentation Software?

Administrative simplification provisions call for the use of standardized, electronic transactions and code sets for submission of insurance claims.

HIPAA states that any practice working with electronic transactions must sent/receive them in a standard format – specifically, the ANSI 837 for claims and 835 for Remittances/Payment Advice. If you use a claims clearinghouse you may not have to modify your system at present to ensure compliance, however you need to make sure that the clearinghouse is compliant with the new regulations. In some cases, you may have to make some modifications to ensure certain HIPAA-required information is captured so that the clearinghouse can create and send a HIPAA compliant transaction. If you currently send paper claims, you may be required to submit claims via Electronic Data Interchange or EDI transactions.*

[* Medicare will require electronic submission except for small practices where there is no method for doing so and where the practice has fewer than 10 full-time employees.]

In addition to standards for electronic transactions for claims, these transactions now have standards specified by the HIPAA for Code sets. Code sets include diagnosis and procedure or CPT codes. If you have been using DSM codes for your claims, you will now be required to start using ICD-9-CM codes.

Standards for Privacy of Health Information are designed to help guarantee privacy and confidentiality of patient medical records.

This regulation requires you to provide information to patients about their privacy rights and how their information can be used, and to secure patient records so that they are not readily available to those who do not need them. Patient authorization is required before a covered health care provider that has a direct treatment relationship with the patient may use or disclose protected health information (PHI).

The HIPAA rules and regulations for privacy cover all forms of data, paper and electronic, and require safeguards for the protection of personal health information. Security standards safeguards to protect confidentiality, integrity, and availability of protected health information and require covered entities to implement basic safeguards to protect health information from unauthorized access, alteration, deletion, and transmission. This would include implementing appropriate password protection, guarding against unauthorized access to computer systems, protecting against viruses and assuring that backup systems are functioning properly.

An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested. The accounting must include the date of the disclosure, name of the entity or person who received the protected health information, a brief description of the protected health information disclosed, and a brief statement of the purpose of the disclosure.

Electronic Signatures

While not currently required by HIPAA, electronic signatures will probably come into effect in the future. Electronic Signatures may be required for persons submitting healthcare claims and claims attachments, and generating electronic medical records or notes using a "digitally encrypted signature". The electronic signature process will require, at minimum, authentication of the signer’s identity and non-alterability after the signature has been applied.

Are DocuTrac Products "HIPAA Compliant"?

DocuTrac products fulfill finalized HIPAA regulations that are required of Practice Management Software. In August 2003, Office Therapy tested and was awarded HIPAA Compliance Certification by Claredi. The Claredi Corporation is the nation’s leading commercial provider of HIPAA EDI compliance testing and certification.

However, no software product, even one that is HIPAA certified, can guarantee that you are HIPAA-compliant. Compliance with HIPAA has as much, if not more, to do with your office policies and procedures in handling protected health information, whether in electronic or paper form. In some cases, protecting data requires the use of additional software systems and implementation of office policies. For instance, the use of Virus scanning software to protect data, or securing passwords used to access software.

How can DocuTrac Products Assist in HIPAA Compliance?

Electronic Claims and Code Sets: The HIPAA ANSI 837 electronic claim and ANSI 835 Remittance format are used for electronic claims in Office Therapy. In addition, clearinghouses recommended by DocuTrac are compliant with regulations.

Office Therapy includes ICD-9-CM codes in place of DSM codes. CPT codes can easily be modified as required.

Electronic Signatures

QuicDoc currently allows for electronic signatures, by providers, for notes and treatment plans. The use of signature pads for digitally encrypted signatures in the Enterprise Edition, in addition to current methods, meets requirements for authentication and non-alterability.

Security and Privacy

Security refers to methods to limit access to and protect confidential data.

QuicDoc has always employed password protection limiting access to the system. Each user has a unique ID and Password to logon, which determines which patient records and areas of the program are accessible for that user. QuicDoc's Enterprise edition adds Role-Based security, and password expiration and renewal options. The latter requires changing of passwords at intervals as specified by the System Administrator.

Since 2001, QuicDoc's database (Standard Edition), which stores patient records, can also be password protected to prevent unauthorized access using another application to open the database. The Enterprise Edition uses Microsoft SQL Server that has very robust security features built-in.

Although password authentication to logon to Office Therapy has been available, it has been optional. It is urged that it be implemented to comply with HIPAA regulations. Database password protection is now available for Office Therapy to prevent unauthorized access using another application to open the database.

Both QuicDoc and Office Therapy have an Audit Log feature to record and track all user activity and actions. The log tracks when, and by whom, patient information is viewed, added, modified, or deleted. In addition, the log will track logon failures.

QuicDoc (Standard Edition) and Office Therapy both have built-in backup/restore functionality. The Enterprise Edition of QuicDoc uses Microsoft SQL Server that has very robust backup/restore features built-in.

Additionally, the use of up-to-date virus protection software, password-protected screen savers, and password logon to the computer is recommended to augment protections listed above.

Privacy

Privacy refers to limiting availability and use of confidential information.

Separate Psychotherapy Notes

The HIPAA privacy rule defines psychotherapy notes as: Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. QuicDoc provides separate Psychotherapy Notes for therapists to keep sensitive information separate from the clients' records. Psychotherapy Notes can be password protected.

Disclosure of Protected Information

QuicDoc and Office Therapy have added a Disclosure of Protected Health Information Log. This allows you to track the date of disclosure, name of the entity or person who received the protected health information, a brief description of the protected health information disclosed, and a brief statement of the purpose of the disclosure.

IMPORTANT NOTICE: DOCUTRAC CANNOT ASSURE HIPAA READINESS OF OLDER VERSIONS OF OUR PRODUCTS.