

Complying with the HIPAA Transactions and Code Sets

This is the sixth fact sheet in a series and is focused on complying with the HIPAA transactions and code set standards. Collectively, the fact sheets will provide information, suggestions, guidance, and checklists to assist you with understanding what you need to do to be HIPAA compliant.

The HIPAA Standards for Electronic Transactions Final Rule published on August 17, 2000 established a standard for conducting certain transactions electronically. These transactions include submitting a claim, receiving a remittance advice, checking a patient's eligibility, checking the status of a claim, and other transactions. The deadline for complying with the final rule was October 16, 2003. The next version of HIPAA transactions will be required for use no later than January 1, 2012. If you are currently using the HIPAA standard transactions, you will need to begin using 5010 version by this date.

When submitted electronically, only the standard format is compliant and may be used. Transactions submitted on paper, through a dedicated fax machine, or via the phone are not subject to the HIPAA provisions. Keep in mind that the Administrative Simplification Compliance Act (ASCA) requires all physicians who bill Medicare to do so electronically according to the HIPAA standards, although physician practices with fewer than 10 full-time employees are exempt.

This final rule also named standards for code sets used to encode data that is sent in the HIPAA-named transactions. Code sets are identified as "medical", including ICD-9, CPT[®], and HCPCS, and "nonmedical," which are administrative code sets, such as ZIP code, state abbreviations, and administrative billing code sets (e.g., place of service). The code sets that are listed or named within a HIPAA-named transaction implementation guide are required to be used.

In addition, this final rule identified "covered entities" as the organizations that are required to comply with the HIPAA-named transactions. Covered entities are health plans, health care clearinghouses, and health care providers that transmit any health information in an electronic format in a HIPAA-named transaction.

The HIPAA Enforcement Final Rule, published on February 16, 2006, sets the requirements related to enforcement of the HIPAA transactions and code sets regulation. The Centers for Medicare & Medicaid Services (CMS) Office of E-Health Standards and Services (OESS) is responsible for enforcing the transactions and code sets regulation and reviewing complaints. Enforcement can include levying civil or criminal penalties. As of February 2010, 652 complaints had been filed and 624 had been investigated and resolved. Complaints for HIPAA security and privacy regulations are managed separately and are investigated by the Department of Health and Human Services (HHS) Office of Civil Rights.

What is Required of Physicians Who are HIPAA "Covered Entities"?

Under HIPAA, providers (including physicians), clearinghouses, and payers are all "covered entities" and thus are impacted by the law. The HIPAA transactions and code sets regulation does not require physicians to conduct the HIPAA-named transactions electronically, however, *if* a physician conducts a HIPAA-named transaction electronically, then the HIPAA standard transaction must be used. The specific requirements are:

[®] CPT is a registered trademark of the American Medical Association

- If a covered entity conducts one of the HIPAA-named transactions electronically with another covered entity, they must use the HIPAA electronic transaction.
- If a physician requests a payer to conduct a HIPAA-named transaction using the HIPAA transaction, then the payer must do so. The payer may not delay or reject a transaction because the transaction is in the HIPAA format.
- Payers must accept and process codes from HIPAA-named codes sets when they are contained within a HIPAA-named transaction.

What is the Compliance Process?

At this time, the compliance process for the HIPAA transactions and code sets regulation is complaint-driven. When CMS receives a complaint about a covered entity, they notify that entity that a complaint has been filed against them. The covered entity then has an opportunity to demonstrate that they are in compliance or submit a corrective action plan for how they will become compliant. Covered entities that are the subject of a complaint must cooperate with the CMS investigation, which may include providing relevant policies or procedures and information related to the complaint.

When a complaint is resolved, the covered entity that is the subject of the investigation and the person who filed the complaint are notified of the outcome. If a covered entity makes reasonable efforts to correct the identified problem and become compliant, they are unlikely to be assessed any fines or penalties.

Who Can File a Complaint?

Any person who believes that a covered entity is not complying with the HIPAA transactions and code sets regulation may file a complaint. If a covered entity refuses to conduct a HIPAA-named transaction in a compliant format, you can file a complaint against them.

How Do I File a Complaint?

The following two websites can be used to file a complaint against an organization that is not following the HIPAA transactions and code sets requirements.

- AMA: www.ama-assn.org/go/clickandcomplain
- CMS: www.cms.gov/Enforcement/Downloads/HIPAANon-PrivacyComplaintForm.pdf

Complaints must be filed within 180 days of when the person filing the complaint became aware of the violation.

What Information Do I Need to Report in a Complaint?

The information that needs to be reported in the complaint includes:

- Your contact information, i.e., name, organization name, address, phone number;
- Information about the covered entity you are filing the complaint against, i.e., organization name, contact name, address, phone number;
- Date when the violation occurred;
- Description of the complaint, including any documentation that supports the complaint;
- Your signature; and
- Additional optional information, such as the type of complaint, the specific transaction, and the specific code set.

Names and other identifiable information in the complaint are kept confidential by CMS, unless the information is necessary for the investigation. Per the enforcement regulation, a covered entity cannot retaliate against an organization or person for filing a complaint.

Examples of Noncompliance

Despite the October 2003 compliance deadline, some organizations have still not implemented all of the HIPAA-named transactions and/or code sets. The following are examples of noncompliance by payers.

- A physician practice electronically sends to a payer a HIPAA-named transaction, such as a claim, request for eligibility, or request for claim status, and the payer refuses to accept it.
- A physician practice requests that the payer electronically send them a HIPAA-named transaction, such as the health care claim payment/remittance advice or eligibility response, and the payer refuses to do so.
- A payer continues to use their own proprietary codes when there is a HIPAA-named code set that must be used.

Understanding what is and is not HIPAA compliant will ensure that you are meeting the requirements of the HIPAA transactions and code sets regulation. You should also know when another covered entity with which you are doing business is not complying with the requirements. Resolving compliance issues you have with other covered entities will improve the efficiencies of conducting your administrative transactions electronically.

Upcoming HIPAA Dates:

January 1, 2012 – Compliance with version 5010 transactions

October 1, 2013 – Compliance with ICD-10 code sets

**Visit the AMA's website for more resources for
implementing the HIPAA 5010 transactions.**

www.ama-assn.org/go/5010