

HIPPA COMPLIANCE Guidelines

Penalties

Non-compliance can result in steep penalties for your organization. Penalties for non-compliance will result in civil and criminal punishment. Fines can be up to \$25,000.00 for multiple violations of the same standard in a calendar year. Fines can be applied up to \$250,000.00 with possible imprisonment for up to 10 years for knowingly misusing individually identifiable health information.

General Penalty for Failure to Comply:

- **Each violation will result in a \$100 penalty. For example, sending a claim file in a non-standard format (such as those used currently) or using a non-standard payer-assigned identifier.**
- **The maximum penalty for all violations of an identical requirement may not exceed \$25,000 per year. For example, 250 non-standard claim files or proprietary identifiers would add up to the \$25,000 yearly maximum. There are as few as 15 and as many as 30 different standards named by HIPAA, and the potential penalty can grow quickly to more than \$500,000.**

Wrongful Disclosure of Individually Identifiable Health Information:

- **Wrongful disclosure offense will result in a \$50,000.00 penalty, imprisonment for not more than one year, or both.**
- **Offense under false pretenses will result in a \$100,000.00 penalty, imprisonment for not more than five years, or both.**
- **Offense with intent to sell information will result in a \$250,000.00 penalty, imprisonment for not more than 10 years, or both.**

Deadlines

Most entities have 24 months from the effective date of the final rules to achieve compliance. Normally, the effective date is 60 days after a rule is published. The Transactions Rule was published on August 17, 2000; changes have been made to these. Visit the **US Department of Health and Human Services** for more information.

Some General Comments

- **Privacy:** To protect patient data from inappropriate disclosure or use.
- **Security:** Safeguards throughout patient information systems preventing unauthorized access.

- **Administrative Simplification:** Administrative standards will replace the numerous non-standard formats currently used for transactions with a single uniform set of electronic formats.

There are three areas to be standardized:

- **Identifying data:** In order to support standard transactions, HIPAA mandates the use of unique identifiers for: providers, all payers, employers, and individual (patient) identification information. The unique identifier for providers is proposed to be the National Provider Identifier (NPI), a 10-digit number. The employer identifier is based on the Internal Revenue Service assigned Employer Identification Number (EIN), a nine-digit number. Payer identification will be 10 digits. The proposed patient identifier will consist of approximately 10 numeric digits with a check digit. Guidelines for Implementation of the standards can be found at the [Washington Publishing Company Web site](#).
- **Code Sets:** ICD-9 codes (diagnosis codes), CPT codes (procedure codes).
- **Transaction Sets:** Health claims (encounters), claim payment and remittance advice, healthcare claim status, referrals, electronic eligibility information, healthcare enrollment, health plan premium payments, first report of injury, and claims attachments.