Everything You Need to Know About **HIPAA Rules for Medical Billing**

Medical billing companies must access protected health information (PHI) to perform their duties, making them HIPAA business associates. As this is the case, medical billing companies must be HIPAA compliant. So, what are HIPAA rules for medical billing?

HIPAA Security Rule and Medical Billing

The HIPAA Security Rule applies to medical billing companies concerning how they protect the PHI to which they have access. Medical billing companies must implement administrative, physical, and technical safeguards to maintain PHI's confidentiality, availability, and integrity.

The required safeguards are as follows:

- **Physical Safeguards:** Protect the physical security of your offices where PHI or ePHI may be stored or maintained. Common examples of physical safeguards include alarm systems, security systems, and locking areas where PHI or ePHI is stored.
- **Technical Safeguards:** Protect the cybersecurity of your business. Technical cybersecurity safeguards must be implemented to protect the ePHI that is maintained by your business. Examples of technical safeguards include firewalls, encryption, and data backup.
- **Administrative Safeguards:** Ensure staff members are adequately trained to execute the security measures you have in place. Administrative safeguards should include policies and procedures that document the security safeguards you have in place, and employee training on those policies and procedures to ensure they are correctly executed.

HIPAA Privacy Rule and Medical Billing

The HIPAA Privacy Rule applies to medical billing companies concerning how they are permitted to disclose PHI to other medical entities.

Medical billing companies may have access to PHI, including:

- Treatment information, including past and current medical conditions
- Fees that patients or their insurance companies paid for treatment
- The location of the treating healthcare provider

Preventing Medical Healthcare Fraud and Abuse, Administrative Simplification, and Medical Liability Reform (Title II)

Title II applies directly to medical billing companies as it dictates the proper uses and disclosures of PHI, and simplifies the processing of claims and billing. Title II also provides guidelines for keeping and sharing electronic records between healthcare entities.

Additionally, under Title II, the Office of the Inspector General (OIG) is in charge of investigating and prosecuting healthcare provider and insurance company fraud.

OIG Compliance

OIG ensures that medical billing and coding companies are not acting fraudulently.

The most common ways medical billing and coding companies commit fraud are:

1. **Upcoding:** Occurs when providers try to get more money from insurance companies for billing patients for services they did not perform.
2. **Undercoding:** Occurs when providers intentionally leave out codes for services provided, intending to avoid an OIG investigation.
3. **Unbundling Codes:** Occurs when providers submit separate claims for services that can be submitted as one bill. This is done in an attempt to maximize payments received from insurance companies.
4. **Falsifying Medical Records:** Occurs when providers falsify patients' medical records, by altering medical histories, payment histories, or descriptions of treatment.

The Surprise Medical Bill Law

The "No Surprises Act" went into effect on January 1, 2022, but the final rules and details of the law weren't released until August 2022.

The final rules issued by the Department of Labor and the Department of Health and Human Services provide a framework for the arbitration of disputes between providers and health plans.

The rules also specify the following:

1. If a qualifying payment amount is based on a downcoded service code or modifier, a plan or issuer must provide the following information with its initial payment:
   • A statement that the service code or modifier billed by the provider, facility, or air ambulance service was downcoded
   • An explanation of why the claim was downcoded, including a description of which service codes or modifiers were altered, added, or removed, if any
   • The amount that would have been the qualifying payment amount had the service code or modifier not been downcoded
2. Independent dispute resolution entities must be certified. They must consider both the qualifying payment amount and all additional permissible information submitted by each party to determine which offer best reflects the appropriate out-of-network rate. After weighing these considerations, independent dispute resolution entities should select the offer that "best represents the value of the item or service under the dispute."
3. Independent dispute resolution entities must explain their payment determinations and the underlying rationale in a written decision submitted to the parties, HHS, and the Labor Department.

A fact sheet from the Department of Labor is available on their website for a more detailed summary of the final rules. Visit: https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/our-activities/resource-center/faqs/requirements-related-to-surprise-billing-final-rules-2022.pdf

---

Compliancy Group. Compliancy Group's simplified software and Customer Success Team remove the complexities and stress of HIPAA, helping healthcare professionals quickly achieve HIPAA compliance. They give healthcare businesses confidence in their compliance plan, increasing customer loyalty, and profitability while reducing risk.
https://compliancy-group.com/