

Compliance in Medical Billing

Compliance is defined as "being in accordance with a wish, request, demand or rule." That covers a broad spectrum. In medical billing, compliance can mean everything from being in accordance with recommended practices to not violating federal law. It is not surprising that there is often confusion about what compliance really means to a biller. In this article some common compliance questions are provided related to medical billing clients and relationships with them.

One of the foundations of any compliance discussion is the Office of Inspector General's (OIG) Model Compliance Plan. It was designed to protect both the provider/client and the billing company. Each party should review the other's compliance plans and ensure that they are both following compliance guidelines addressing unbundling, upcoding, etc. Routine monitoring and auditing by the billing company should reveal potential problems by the provider/client or within the billing company. If problems are discovered, the compliance plan guideline should be followed for reviewing, discussing, training and reporting errors potentially leading up to termination.

Must my clients have a compliance plan? If not, can we provide one for them?

In the guide from the OIG regarding Model Compliance Programs it is stated that billing companies and medical practices should have an active compliance plan; however, it is not mandatory. While the billing company compliance plan may not act as a substitute for a medical practice's own plan, the company may assist a client in developing its own plan. If a client does not have a compliance plan, or is not actively working to develop one, the billing company has the responsibility to notice patterns of abuse and should work with the client to rectify the situation.

Are we responsible if a client refuses to process refunds?

Federal law allows for the prosecution of anyone that does not refund overpayments. As indicated in the OIG Model Guidance for Third Party Billing Companies, we have a responsibility to notify our clients of overpayments and assist with their compliance to both Federal and State refund requirements. A billing company can be found culpable as a co-defendant or co-conspirator if they were aware or should have been aware of a client's failure to process refunds. If the billing company fails to notify clients about overpayments, the billing company could become the primary defendant. Federal criminal prosecution can result in a \$25,000 fine and up to ten years in prison per item.

If my client supplies the CPT codes for services performed are we responsible for errors or is the client?

Whether the client or the billing company assigns CPT codes, providers remain primarily responsible for the accuracy of their claims. To protect their interests, providers should require their billing companies to provide written warranties that they will exercise diligence, care and integrity when submitting claims for payment for services rendered, and will maintain honest, fair and accurate billing practices. Furthermore, providers' billing companies should warrant that their personnel are knowledgeable and sufficiently trained to perform all claims development and submission functions in strict accordance with federal and state laws, regulations and protocols, and all other third party payor requirements.

Can we bill physician charges if they don't provide their reports or chart notes?

To maintain compliance, billing companies should submit claims only when appropriate documentation is provided to support the claim in an organized and legible format, and one which can easily be audited and reviewed.

Can a medical provider offer a discount to an uninsured patient?

According to the OIG, a medical provider can offer discounts to uninsured patients as long as the discount is consistently applied and is not related to any inducement for referrals.

Can a medical provider offer professional courtesy?

Yes. According to CMS professional courtesy can be offered to a physician, their immediate family member or office staff if there is a written policy and it is not related to any inducement for referrals. Details can be found at 42 CFR Section 411.357(s).

How many patient accounts, charts or reports must we monitor and audit each year?

The OIG Model Compliance Plan suggests that regular monitoring and auditing is an integral part of a compliance plan, and has indicated that a sample as small as 1% is sufficient. When determining your monitor/audit percentages remember to take into consideration that the sample should be small enough that you will consistently perform the task, yet large enough to be statistically valid and reveal any deficiencies. Monitoring and auditing can be performed on a daily, weekly, monthly or quarterly basis depending on the volume of work as long as it is done on a regular basis. The documentation can be as simple as completing and retaining a form with the following information:

- The Date of Audit/Review
- The Number of Accounts, Charts or Reports Reviewed
- A Report of the Findings (e.g. Reviewed 20 accounts. No problems found.)
- The Action Taken as a Result of the Review
- The Name and Signature of the Reviewer

How do I select patient account, reports or charts for auditing?

Internal audits should be performed on a random sample that can be selected through any number of criteria such as by physician, location, type of service, employee or date of service. After performing a thorough risk analysis of the billing company or medical practice to identify threats, vulnerabilities and risks to the organization, the results can then be used to identify the areas of greatest risk and direct you to the specific areas that need to be audited and monitored.

We receive our patient demographic and charge information electronically from our clients' locations, and receive some Protected Health Information (PHI) by email.

How does that need to be protected to avoid exposing PHI?

The HIPAA Security Rule states that we must implement the necessary safeguards to protect patient health information regardless of how the PHI is sent, delivered or stored. Your Risk Assessment, Compliance and HIPAA plans, and Business Associate Agreements should address the transport of PHI electronically to meet the guidelines as detailed in the Federal Register/Vol. 74, 162 dated August 24, 2009. Considering the tools available, encryption of demographics, charges and email should be considered standard of care. If a business partner, employee or client refuses to encrypt an email containing PHI, the billing company should follow the procedures outlined in its Compliance Plan. This should begin with training and discussions possibly leading to dismissal of the employee or client.

What precautions should be taken when physically transporting PHI?

After performing a risk analysis to determine vulnerabilities, policies should be established to address those circumstances. This should include transporting the data containing PHI in a closed, lockable, marked container like a briefcase or suitcase. The billing company's Emergency Plan should include a section covering transport risks like theft or accidents.

Courtesy: *HBMA*