Part B Insider (Multispecialty) Coding Alert

Privacy: Know What Identification Theft Can Mean for Your Part B Practice

Just one infraction can shut down a small practice and put you out of business.

If you don't follow privacy compliance regulations you might face civil liabilities and criminal charges as well, experts say. Check out the following information for determining how any of these issues could impact your practice.

Medical ID theft can wreak financial havoc for providers and facilities. It can be considered a violation of provisions of the HIPAA Security Rule and may lead to complaints to the Office for Civil Rights of the Department of Health and Human Services that, in turn, can lead to proceedings for civil monetary penalties, warns **Kenneth Rashbaum, Esq.** of Rashbaum Associates, New York, N.Y. These penalties can reach hundreds of thousands of dollars or more. State attorneys general may bring HIPAA proceedings, and they can also bring actions to enforce state privacy and anti-identity-theft laws.

Employees take the heat: "In addition, there are criminal sanction provisions in HIPAA, and these have been used in the past to prosecute identity theft from hospital patients," Rashbaum points out. "No hospital wants to be in the news for a criminal prosecution of an employee," he adds.

All of this adds up to "the likelihood of a very real negative impact on the provider or facility's goodwill," says **Jim Sheldon-Dean**, Director of Compliance Services with Lewis Creek Systems, LLC in Charlotte, Vt.

If it's a reportable breach under HIPAA, the costs of notification can be significant, both in dollars and in public trust, since the fines can be assessed on a daily basis, up to $1.5 million in a year for any one provision violated, Sheldon-Dean goes on to say. There are also likely to be ramifications under state breach notification laws, and for some institutions the FTC's Red Flag Rule applies, he adds.

Real Losers When Medical ID Is Lost

"The biggest problem with medical ID theft is not only the cost to all of the stakeholders that lose money which cannot be recouped," but the patient, whose identity has been stolen pays a price as well, says **Ester Horowitz, CMC, CITRMS, CIISA.** Patients may have two records in their name -- the real one and the fake one used to get drugs or treatments, she adds.

Health hazard: Confusion over identities can seriously jeopardize patients' care. Identity theft poses "a danger to the patient's wellbeing when the medical system is contaminated with wrong information making it difficult to treat the patient in emergent situations," Horowitz warns.

EMR trust erosion: Loss of trust in the EMR and, by implication, in the provider can be another fallout, warns Rashbaum. If patients cannot trust the EMR, that loss of trust can bring about loss of patient base and a significant loss of revenue, he points out.

Bottom line: Thwart security threats by using the strategies outlined in Vol. 13, no. 13 of the Insider. To access that and all archived issues, visit https://www.aapc.com/codes/.