Health Information Compliance Alert

Security Compliance: Don't Wager On HIPAA To Protect Patient Privacy At The Bank

But making the bank a business associate can temporarily safeguard your PHI.

Do you send your patients' protected health information (PHI) to your bank along with your claims? Can your patients expect their private medical information to remain protected? The resounding answer is "No."

There is a huge tug of war being waged on whether banks are responsible for protecting patient privacy, and privacy may be on the losing end of the stick, experts tell **Eli.**

Though banks often act as clearinghouses for healthcare providers, the banking industry is working to exempt itself from the Health Insurance Portability and Accountability Act (HIPAA) umbrella. At a hearing before the National Committee on Vital and Health Statistics, the banking industry testified that the HIPAA regulation directly conflicts with the various other regulations with which banks must comply.

Problem: The regulations were never coordinated, and so it is likely that the banking regulations and the healthcare regulations stand in direct contrast to each other.

Solution: Bank regulators and HIPAA regulators have to get together and work this out.

Banks Become Business Associates

Banking groups like the **American Banking Association and the Electronic Payments Association** have stated that banks can meet their HIPAA obligations via a business associate agreement (BAA), making any further HIPAA compliance unnecessary.

"It's not clear that BAAs provide an appropriate level of [patient privacy] protection," explains **Anna Slomovic,** a senior fellow at the **Electronic Privacy Information Center** (EPIC) in Washington, DC.

Warning: "The banks are going to be transmitting information to other banks. Once the data moves outside the HIPAA protection regime, there is no more protection," she clarifies. That means that as soon as your patient's information goes into the banking system, it is no longer safeguarded by HIPAA's privacy and security rules. While there are personal privacy protections set forth in banking regulations, none of them produce the same effect as HIPAA.

Example: The Financial Modernization Act, also known as the **Graham-Leach-Bliley Act** (GLB), allows banks to share a client's information. This "record sharing" is "what we don't want in the case of health information," Slomovic asserts.

Though complying with HIPAA puts a tremendous burden on banks, it would enable the **Office for Civil Rights** (OCR) to "come down directly on them for violations, unlike a BAA in which banks are only subject to potential termination for their contract," clarifies **Deborah Larios,** a partner in the Nashville, TN office of **Miller & Martin.** The risk of penalties would force banks to implement policies and procedures to protect PHI at all stages of a transaction, she says.

What's Good For the Goose...

Banks' involvement in the healthcare industry isn't a foreign concept. A clearinghouse is the channel through which providers and health plans operate, explains **Matthew Rosenblum,** COO of **CPI Directions, Inc.** in New York. Due to the cost of using a clearinghouse, many providers rely on banks to transfer bundled electronic claims and funds to the appropriate destination.

Why: "It's a natural business for banks to get into -- they already have the computers, technical expertise and people-power" to facilitate clearinghouse functions, Rosenblum states. And when a bank performs clearinghouse functions, those bank components must comply with HIPAA regulations.

So why is the banking industry fighting tooth and nail to avoid the clearinghouse label? It's all about cost, experts agree. "If you look at the rules for clearinghouses, an entity that is both a bank and a clearinghouse has to separate out clearinghouse functions and set [those functions] up as a HIPAA entity," Slomovic explains. That's not cheap!

As it stands, banks are in major competition with clearinghouses because they do not have to put forth the same financial efforts as the latter.

Tip: This financial freedom allows banks to offer their customers a greater return than clearinghouses can. "If [banks] don't have to spend any extra money on HIPAA compliance," they can offer their customers both savings and a value-added service, Slomovic says.

Mining For Data

The healthcare industry is concerned about the many ways banks' HIPAA exemptions will affect patient privacy for several reasons. The most important reason is also the most obvious. "Privacy protection leads to better healthcare because people trust the system more," Slomovic reminds. "Making banks fall under HIPAA will provide better healthcare" through stronger patient-provider relationships, she asserts.

Caveat: As patients' PHI becomes more closely bound with financial transactions, the ability of data miners to extract and use that information increases. A senator's wife goes to a substance abuse specialist and pays with a credit card, Rosenblum postulates. "Somebody in the bank gets this information, notices it's the senator's wife and suddenly that information is leaked to the press," he explains.

While you are under no obligation to warn your patients of the risk posed to their privacy by the involvement of banks, you might find that patients welcome the heads up. You have to "weigh the danger of scaring the patient away" against the likelihood that they'll appreciate the information, Larios says.

Suggestion: If your patient is receiving treatment for a sensitive issue, you may want to let them know about the risks involved because "very sensitive information could be misused," Larios warns. Though this may change patients' decisions about how they receive their healthcare, it will also instill trust and confidence in the patientprovider relationship, she says.