Health Information Compliance Alert

HIPAA Privacy: PRIVACY REGS YOU CAN BANK ON

Special services rendered by banks on behalf of providers and hospitals could emerge as an unheralded HIPAA compliance time-bomb.

The growing symbiosis between banks and providers can have adverse consequences for bankers who lack a firm grasp of their responsibilities under the Health Insurance Portability and Accountability Act's privacy rule and, as an April survey showed, banks are still unprepared for HIPAA (see HICA, vol. 2, no. 4, p. 38). But as it turns out, providers can help banks maintain compliance by carefully scrutinizing the information they send to them.

Banks often receive electronically transferred payments from insurance companies sent straight from a payor to a bank. These transactions generally include two parts: the payment portion; and the electronic remittance advice (ERA), which refers to a document containing protected health information.

Banks need not be concerned with the electronic funds transfer (EFT), even though that document includes information about the payor, the payee, the amount, the payment method, and a reassociation trace number. Since the EFT contains no individually identifiable health information, HIPAA doesn't become an issue of concern.

It's the ERA that bankers need to look out for, says **Deborah Larios**, an attorney in the Nashville office of **Waller Lansden**. If the bank receives that information but doesn't use it, they have nothing to worry about. However, if they do anything with the information, such as read the data or translate it out of its electronic format, then they suddenly become subject to HIPAA's privacy rule, she notes.

The ERA contains specific information about the patients and the medical procedures for which the money is being paid and is used to update the provider's accounts receivable system, according to the preamble to the final privacy rule. Such information is always required in order to complete a health care payment and remittance advice transaction.

Larios explains that some banks only receive the payment portion from a provider or hospital, and in those cases they're not subject to HIPAA. Similarly, receiving both parts doesn't necessarily inculpate them either, since leaving the ERA encrypted and forwarding that information straight on to a client just means banks are simply acting as couriers.

But it's when banks alter that data on behalf of their clients even to the slightest degree that HIPAA becomes an issue, since then banks have metamorphosed into a business associate, says Larios. When that happens banks would need to sign a special agreement with the provider client and would be required to implement safeguards and promise never to use that information for certain purposes.

And according to the preamble to the privacy rule, a bank that operates the accounts payable system or other "back office" functions for a covered health care provider would meet the definition of a business associate, thus mandating a business associate contract with the bank before any disclosure of PHI is made.

Generally, whenever banks have access to individually identifiable health information, they'd be under the jurisdiction of the **Department of Health and Human Services** for enforcement of HIPAA, says **John Casillas**, founder of Franklin, TN-based **Medical Banking Project**.

Casillas says one of the common services provided by banks where HIPAA applies includes treasury management or cash dispersal services. For example, a health plan may contract with a bank. The bank becomes the outsourcer for the health plan's accounts payable department, and the latter adjudicates claims. The health plan sends a proprietary payment file to the bank the file contains both payment instructions and remittance information and the bank processes those transactions based on the preference of the provider.Whenever the banks receive the proprietary payment file, that

bank has just become a business associate and subject to HIPAA, says Casillas.

Another area that frequently impacts banks concerns something banks may not even know about. Every community hospital that receives payments from an automated clearinghouse may routinely and oftentimes unwittingly receive PHI. If a bank has access to PHI for ACH transactions, "then the provider needs to form a business associate agreement with the bank," says Casillas. That data is protected under HIPAA, he warns, even though the hospital may just throw that information away.

Banks As Clearinghouses

But what happens when banks receive the standard electronic form (the ERA) from the payor and then translate that form "into English" from its electronic format? Those situations are a little more perplexing, Larios maintains. She says there are a lot of banks that like to perform many "back office" services for provider clients, such as collecting money either in electronic or paper form, and helping the physicians or the hospitals post it to the proper account.

Occasionally, banks won't stop there. Larios says banks often will transfer the wired money to the correct account, take the ERA that came with it, and then tell the physician or hospital how much money was posted to their client's account. Sometimes banks will then tell the provider or hospital to include in their accounts that their client's bill has been paid.

At that point, the bank is doing something different, Larios maintains. By translating that standardized electronic information into some other form, even if it's just putting the information into words rather than it's original electronic format, banks have altered the information. Abracadabra: "They then become a clearinghouse and a covered entity under HIPAA," says Larios.

Casillas explains that the proprietary payment file comes into play here too. Whenever banks receive a proprietary payment file, they become a business associate under the privacy rule. Additionally, when banks convert that payment file into a standard, then they fit the definition of a health care clearinghouse, with the right to be enforced under HIPAA.