Convenience vs Compliance: How Much Is It Costing You?

Federal law requires that rural health clinics (RHCs) are HIPPA compliant. An RHC could face stiff fines and penalties if they are not compliant or if there is a breach. In today's age of electronics, many RHCs are already using the various EHR/EMR programs that are available to them. Each of these software companies claim to offer the best features and benefits, the most obvious being that they are HIPAA compliant. In an effort to stand out amongst the competition, many offer direct integration merchant services capabilities. How great is it to swipe a patients' card, enter the dollar amount, and have the transaction post on the patients' chart?

If you accept credit/debit cards as a business, the major card brands really want you to be Payment Card Industry Data Security Standard (PCI DSS) compliant. PCI compliance, like HIPAA, is designed to protect personal data; however, it is not "law." Businesses can still be assessed various penalties; I have seen them as high as $89 per month if they don't meet the criteria of their merchant services company. Usually, an electronic scan and the completion of a Self-Assessment Questionnaire (SAQ) is required.

If you are using an "all inclusive" EHR/EMR software program, take a look at your merchant processing statement and see if you are being charged a Non-PCI Compliance fee. If so, find out why. Does your software program not permit an external scan? Are the SAQ questions so convoluted that you cannot answer them?

Then ask yourself, I have to manually post cash and check payments, so can I take another few seconds and post the card payments as well? Or do I want to keep giving my processor extra money?

Rich Williamson
USPAY
richw@uspay.com