Health Information Compliance Alert

Reader Question: What Is '2-Factor Authentication' & When Must You Use It?

Question: There's some confusion in our medical office regarding what "two-factor authentication" means and when we need to use it. Can you explain?

Answer: "Two-factor authentication" (also known as "dual authentication," "two-step authentication" or "multi-factor authentication") means the use of more than just a password and user name, explained attorney **Mary Beth Gettins** of **Gettins' Law** in a recent blog posting.

Definition: Two-factor authentication is a technology that provides identification of users by means of the combination of two different components, which may be something that the user knows, something that the user possesses, or something that is inseparable from the user.

Examples: When you make a withdrawal at the ATM, you typically need to provide an ATM card (something you have) and a PIN number (something you know), Gettins said. Or, when you need to reset or set your password, you may receive a code via text message (something you know) to your phone (something you have) after entering your user name. These are both examples of two-factor authentication.

You should use two-factor authentication for high- or higher-risk access to information, Gettins advised. For instance, you should use two-factor authentication for:

- Remote access to information;
- Access to highly private information or financial information;
- Resetting passwords; and
- Changing the computer configuration.