Privacy & Security Updates

February 2010

Share your workstation, not your password

Has a co-worker ever asked to borrow your username and password to quickly look up patient information because she has forgotten her own? Have you ever walked up to a workstation, found that the previous user hadn’t logged out, and decided to just look up the information you needed instead of logging in as yourself? Did you know that these situations put you and Providence at risk?

Providence employees are issued unique login credentials, also known as a username and password, to access our computer systems and perform functions such as job-related duties, submitting work hours for payroll and enrolling in benefits programs. The combination of a unique username and password provides confirmation to our systems that the person logging in is really you.

Your username and password provide you the right level of access to electronic information to do your job. For example, a clinician and an accounts manager may both have permission to access patient information, but their unique credentials determine the specific type of information they may view.

Additionally, our individual credentials keep us accountable for our actions. Each time information is entered into our systems or a Web site is visited, the username, date and time are logged. If there were ever an issue at a later time, these logs could be reviewed and, if appropriate, the individual would be held responsible for actions performed using his username and password. The HIPAA Security rule also requires an audit trail for all users so we can determine who is accessing protected health information.

Use a strong password and never share it with others
Keep these guidelines in mind when creating your password:

- Don’t use words found in a dictionary or personal details such as your birth date, family or pet names, favorite sports teams, etc.
- Use at least eight characters
- Use a mixture of uppercase and lowercase letters with numbers
- Periodically change your password