Best Practices for Cyber Security in the Healthcare Field

written by CPH Insurance | June 15, 2016

Cyber security is a hot and incredibly pertinent issue in the mental and allied health field today. With the common use of electronic health records and multiple points of access to sensitive health information, it's more and more important that healthcare groups, big or small, stay protected.

Anti-virus software

Most attackers get into computers via viruses and exploiting coding vulnerabilities. Make sure that the product you are using stays continuously updated. It's an easy write off and a small price to pay for security.

Ultimately, the most important part of your security is to control access to any information that may fall under HIPAA compliance regulations.

Set permissions for which users can access sensitive data. To keep your electronic health records, or EHRs, safe, it's important to make sure that the ability and methods of access are extremely controlled.

Strong Passwords

2014 has marked several exceptional breaches of security for all groups. This leaves members of the healthcare field exposed to double the amount of risk: both personal information, and professional, HIPAA compliance threats.

Strong passwords have a purpose – it may seem obvious, but no matter what a strong password can slow down hackers from getting into your system.

What this means: never leave a computer exposed. Even your personal computer should have a password to log in, no matter if it's a laptop or a desktop that stays at your home at all times.

The Dos and Don'ts of strong password security:

DO NOT:

-use words found in the dictionary, even if they are altered with letters and numbers

-use personal information, such as birth dates, names, pets, SSN, etc.

-use passwords that you already use on social media/social networking sites

DO:

-make a password of 8+ characters in length

-use upper and lower case letters

-use at least one number

-use at least one special character

-change your password on a regular basis

Implement measures for forgotten passwords

To prevent people from writing down their hard-to-remember, rotating passwords, make sure that you have a backup plan. This can include:

-Storing hard copies in a safe

-A few high-security staff members with administrative privileges who can add, delete or reset passwords.

-Implementing a security program that can allow for password recovery.

Use multi-tiered security to authenticate access

Don't just require a username and password to log in to major business accounts and computers. This can include a key fob, a smart card, a fingerprint scan, or photo key identification.

Ultimately, there is no way to prepare for the worst. That's what professional liability insurance is for. Prevent future problems and be ready by staying covered under a liability insurance plan.

Still not sure how to best prepare for the worst? Visit HealthIt.gov to discover more best practices in cybersecurity