Your Software and Devices Are Not HIPAA Compliant

written by CPH Insurance | June 15, 2016

With growing frequency, vendors market their software, devices, and services as “HIPAA Compliant”. This feeds into the mistaken belief that such beasts exist. It’s somewhat understandable. After all, it’s must easier to say “Our cloud-based software is HIPAA compliant” than to say “As a Business Associate, we adhere to all the rules and regulations of HIPAA and HITECH and will sign a Business Associate Agreement with you in order to help you maintain compliance as a Covered Entity. There are, of course, multiple other things you need to do to maintain compliance that we can’t necessarily help you with.”

So, while you may participate in the marketing speak in the interest of easing communication, it’s important to note that there is no such thing as compliant software or a compliant device. Put another way, you cannot maintain HIPAA compliance by simply “only purchasing HIPAA compliant stuff”. Only Covered Entities and Business Associates can be compliant. They do so by following all of the requirements of HIPAA and HITECH, which are extensive when it comes to technology. With the deadline passed for complying with the latest update to HIPAA, it’s more important than ever that Covered Entities ensure compliance.

There are multiple pieces to establishing and maintaining compliance. Especially with technology, you must establish administrative, technical, and physical safeguards that follow HIPAA/HITECH requirements. The short summary is that:

- Administrative safeguards refer to doing a risk assessment/analysis and establishing policies and procedures regarding the creation, storage and transfer of PHI and ePHI (electronic PHI) (Policies can address who has passwords/access to PHI and much more) Technical safeguards mean you use technical means to secure the data (for example, strong passwords and encryption)
- Physical safeguards mean you use physical means to protect the data. (for example, keeping devices in a secure location when not in use and restricting who has access).
- As always, where HIPAA is concerned it is important that you Document, Document, Document. Should you ever be audited or investigated, your documentation that you’ve done due diligence will likely play an important role.

There’s a lot more to each of the three steps above.

Rob Reinhardt, LPCS

http://www.tameyourpractice.com

Rob is a Licensed Professional Counselor Supervisor in private practice and owner of Tame Your

Practice, which provides comprehensive business and technology consulting to mental health and wellness professionals.