Security

Technology, Information Technology

Security Security I agree with the first and third claims made by the healthcare IT staff. The certification criteria used by HIPAAto justify and fund the shift from paper records to electronic ones is also essential.

First, I agree that application-level data security is claimed to be sufficient for HITECH and HIPAA compliance. Application-level data security builds an all-inclusive security program. It is important for healthcare providers to consider and serve in terms of a holistic data security program that integrates security around patient information to hinder its access by unauthorized parties. HIPAA requires such programs to comply with and apply its rough, role-oriented, access control, authorization, and authentication policies. These policies help make sure that patient data is protected appropriately and that healthcare providers adhere to them (Kibbe, 2005). Overseeing and sustaining these kinds of initiatives in an active environment is certainly a heavy burden for healthcare providers. These rules are in some because healthcare providers are equally committed to allocating as much resources as possible to and concentrating on the quality of care given to patients. Translating these functions into a convenient and successful security and compliance initiative is difficult (Kibbe, 2005).

Second, I disagree with their claim that all application-to-database accesses by any healthcare professional are logged automatically. For a healthcare organization to enjoy automatic logging of application to database accesses by doctors, nurses, lab technicians, and administrators, it has to employ additional security and identity management solutions. Unfortunately, HITECH does not cover these additional technological solutions even though

HIPAA requires that all healthcare providers do (Kibbe, 2005). When medical practitioners and other healthcare professionals within a single healthcare organization enter data freely into a secure database through an application-to-database access, links healthcare providers are authorized to access the same data as well. This approach may eliminate redundant paperwork and lower administrative burden, but increases the risk of intrusion by unscrupulous parties in linked healthcare organizations. Ensuring that applicable system events such as booting and rebooting are logged is important because developers have to support the secure conveying of these logs from the applications to administrators. Accesses made by healthcare professionals have to be compliant with regulations imposed across all of the different scaled and levels of healthcare provision and services. Some of the regulations present in the HITECH act and HIPAA are unclear (Kibbe, 2005).

Lastly, I agree that doctors need quick access to EMRs so that encryption and key management overhead, or simply the loss of decryption keys, cannot slow them down. The password for any encoding or decoding system has to be cleared at some point for it to be entered for logging successfully (Terry, 2015). If a user locks the system along with the pass code, the pass code will be retrievable from a different location and time. There appears to be no way to circumvent this requirement. Even though many healthcare providers implementing tectonic medical records, some practices remain slow. In addition, electronic health records with the above encoding and decoding systems are costly, which healthcare providers treat as a key management overhead (Terry, 2015).

References

Terry, K. (2015). EHR Security: To Encrypt or Not To Encrypt. iHealthBeat. Retrieved from http://www. ihealthbeat. org/insight/2015/ehr-security-to-encrypt-or-not-to-encrypt

Kibbe, D. C. (2005). Ten Steps to HIPAA Security Compliance. Family Practice Management 12(4): 43-49.