**Why HIPAA App Security is not Enough for Privacy in the Health Sector?**

HIPAA standard was formulated to regulate privacy and security in the healthcare sector. But it has not been very successful in keeping up with the desired outcomes. The main reason is that the initiators of HIPAA only considered health information to be residing in limited locations like healthcare providers, health information clearing houses and insurance companies. Requirements of HIPAA were only imposed upon these covered entities, thus excluding a wide range of digital healthcare services.

Consumers have now new technologies available to track their health in the form of mobile apps like Apple Watch and Samsung SHealth. Moreover, the use of online health communities and social media is also allowing individuals to manage their health, thus leading to a surplus database of personal health information. This, obviously, was not considered when HIPAA was introduced. It only applies to three major entities i.e. Healthcare providers, health information clearing houses and health insurers. It also encircles business associates that deal with covered entities and exchange information with them. However, companies providing consumer health services like Fitbit or Garmin do not fall under any of the categoriess. Consequently, HIPAA does not apply to any of these setups.

Users of such services, however, do not realize this and consider all health services as HIPAA compliant. Many consumers agree to share their personal health information with mobile health apps, considering these to be falling under the category of “HIPAA covered entitites” and keeping their information private. A study published in Journal of American Informatics Association in 2014 suggests the contrary. According to that, less than one-third of mobile health apps provided security policies. Even out of those apps that do, very few are at the level of HIPAA app security, and most of them have no visible focus on compliance to security standards.

**So what needs to be done?**

Even if HIPAA does include consumer health businesses under the HIPAA compliant covered entity category, it may not be very easy for the latter. Compliance burden will interrupt in the functioning of these businesses due to their limited expertise in the field. Also, it will result in a reduction of services provided to the customers, or an increase in their usage price. If consumer health technology needs to be regulated, it must be done through dedicated laws for this particular niche.

Luckily, we have the **Federal Trade Commission Act** that makes it obligatory for businesses to keep consumer data secure and avoid deceptive strategies. Also, the FTC Health Breach Notification Rule has made it mandatory for specific organizations storing Personal Health Information to notify affected individuals, FTC and media in the event of a breach. This act can further be regulated for ensuring the protection and privacy of PHI on part of entities uncovered by HIPAA.