Defending Patient Breaches for Hospitals

Darshan Talks Podcast

July 28, 2021

On this episode of *Darshan Talks,* we had discussed Health Literacy with guest Krishna Jani. Krishna Jani, Cybersecurity & Data Privacy Attorney at Flaster Greenberg PC, had spoken about the relationship between data privacy, life sciences, and health issues in the legal domain. She had highlighted that healthcare services should ensure that they don't compromise patients' digital privacy in any way. What startups do with patient data matters regarding what legal liability or implications are placed on them. Example: If they sell data for a profit, it might come under California's CCPA or the new CCRA regulations. There are a lot of hospitals getting hacked despite hiring IT teams to avoid these incidents. This is often because they outsource the IT work to another company, have an outdated privacy policy, and don't discuss cybersecurity in board meetings. Besides the breach of privacy to patients, there is also a strong possibility that the hospital will be sued. Thus, hospitals need to hold themselves accountable, focus on data privacy and keep themselves up to date with the latest digital security compliances. She had cited a study in the 80s where people could connect even 1 or 2 data points to a single person. With the advancement of technology that is there now, it is even harder to remain completely anonymous. Thus, it is advisable to delete unnecessary patient data systems for clinical trials or purposes of research and development. A defence would arise only if there has been some substantial effort made or standard of care exercised by hospital management to curb these cybersecurity attacks, even if attacks have become increasingly sophisticated over the years. She had concluded with an interesting point: healthcare data is 3x more critical than financial data.