Cybercrime Newsflash

One major cyber attack that happened recently was in the hospital or medical company of Kaiser Permanente in which there was a huge data breach. More than 13.4 million members of Kaiser Permanente were affected by this data breach[1]. Kaiser's tracking technologies on its website and mobile apps were misused, allowing third-party advertisers like Google, Microsoft, and X (Twitter) to access user data. The data included IP addresses, names, search terms, and user interaction[2]. Kaiser's use of tracking tools have drawn so much backlash in the past. Many of its customers had a bunch of their private data exposed during the cyber attack. When someone's IP address is exposed, hackers can find out where they live based on where the IP address is located. There was so much unauthorized access which caused backlash among its customers. The data of 13.4 million customers was leaked across various social media platforms, and because of this millions of people saw their private data, which violates the social contract theory. The motive was unclear but it could have been used for targeted marketing, criminal proceedings, or discrimination. The breach was caused by the misuse of web technologies, and lack of oversight. The breach caused so much sensitive data to be exposed to the point there was no confidentiality. There was unauthorized sharing of information, even without direct financial or social security details, which potentially violates this trust and the social contract theory. Many patients may not have been aware that their data would be shared with third-party trackers or advertisers, which violates the Deontological ethical theory. There are many ways to prevent this cyber attack or any cyber attack from happening in the future. Kaiser Permenanente should avoid using third-party tracking cookies or data analytics tools that might share sensitive data with external entities. Instead, Kaiser Permenanente can employ privacy-focused tools and anonymize any data necessary for service improvement. Encrypting data at rest and in transit is essential.Conducting routine audits, penetration testing, and vulnerability scans helps identify and fix weak points in security systems.

1. Minemyer, P. (2024, April 26). *Kaiser Permanente reports data breach impacting 13.4m health plan members*. Fierce Healthcare. https://www.fiercehealthcare.com/providers/kaiser-permanente-says-134m-impacted-data-breach

2. *Kaiser's website tracking tools may have compromised data on 13 million customers*. Cyber Security News | The Record. (2024, April 26). https://therecord.media/kaiser-permanente-potential-third-party-data-exposure

3. Votiro. (2024, July 15). *How UHC and Kaiser tackled their cybersecurity ordeals*. https://votiro.com/blog/how-uhc-and-kaiser-tackled-their-cybersecurity-ordeals/#:~:text=Kaiser%20Permanente%2C%20a%20well%2Dknown,attacks%20targeted%20different%20data%20types.