Parking lot USB exercise

Contents	• *The USB device contains both personal and work-related files, including family photos, resumes, employee schedules, and internal budgeting documents. Some of these files contain personally identifiable information (PII), such as names, employment details, and possibly financial data. Mixing personal and professional data increases the risk of unauthorized access and data exposure.* • *Yes, the employee budget, shift schedules, and the resume contain sensitive work-related information. These files could expose internal operations, staffing details, and personal employee data, which could be exploited by a threat actor.* • *No, it is not safe to store personal files together with work files. If the device is lost or compromised, both personal and organizational data could be exploited, increasing the overall impact of a security breach.*
Attacker mindset	• An attacker could use the information on the USB device to impersonate the new hire and gain unauthorized access to hospital systems. Documents such as schedules and internal communications could be leveraged for social engineering attacks against other employees. This information could also be used to target relatives or gain trust within the organization, potentially leading to broader data access.
Risk analysis	• Malicious software such as malware, spyware, or trojans could be hidden on removable storage devices and automatically execute when connected to a system. If an infected device were discovered and used by another employee, it could lead to lateral movement and widespread compromise of organizational systems. A threat actor could access employee data, operational schedules, and internal documents, which could be used for identity theft, surveillance, or social engineering attacks. Technical controls such as endpoint protection, disabling USB autorun, security awareness training, and clear policies on removable media usage could mitigate these risks.*o track what he do for use it for fake his identity*