Parking lot USB exercise

Contents	• *The USB drive contains both personal files, like family and pet photos, and sensitive work files, such as a new hire letter and an employee shift schedule. These work-related documents likely contain personally identifiable information (PII) about employees, which is sensitive and should be protected. Storing personal files alongside work files on the same device increases the risk of accidental exposure and security vulnerabilities, making it an unsafe practice.*
Attacker mindset	• The information on this USB drive could be used to harm both Jorge and the hospital. Personal files, like family photos, might reveal details about Jorge's relatives that attackers could exploit for social engineering or phishing attacks. Sensitive work files, such as the new hire letter and employee shift schedule, contain data that could expose other employees' information, providing a foothold for attackers to infiltrate hospital systems, compromise security, and access confidential business information.
Risk analysis	• To mitigate risks from potentially infected USB devices, technical controls like endpoint protection software and USB port restrictions should be enforced on workstations to detect and block malicious software, such as spyware, ransomware, or trojans that could be hidden on these devices. Operational controls, including regular employee training on secure file storage and the dangers of plugging in unknown USB drives, would raise awareness of the risks associated with personal and work file storage on removable media. Additionally, implementing managerial controls, like a strict policy against storing sensitive work files on unencrypted personal devices, could reduce exposure to sensitive information, which a threat actor might exploit for unauthorized access or social engineering attacks against employees or the organization.