Parking lot USB exercise

Contents	• This device contains a mix of personal and work-related information. Personal files include "Family photos," "Our dog pics," "Vacation ideas," and a "Wedding list," while work files consist of a "New hire letter," "Shift schedules," "Employee budget," and a "JB_Resume." • There are files that can contain PII (Personally Identifiable Information). The "New hire letter" and "JB_Resume" would likely contain Jorge's full name, address, contact details, and potentially social security number or other identifiers. The "Wedding list" could contain names and potentially addresses of friends and family. • There are sensitive work files. "Shift schedules" could reveal staffing levels, employee movements, and operational vulnerabilities of the hospital. "Employee budget" might contain financial data, department spending, or project allocations that are confidential. • It is generally not safe to store personal files with work files, especially on an unsecured device like a USB drive. This practice blurs the lines between personal and professional data, increasing the risk of sensitive work information being exposed if the device is lost or compromised, and potentially violating company data policies.
Attacker mindset	• This information could be used against Jorge through identity theft (using PII from his resume or new hire letter) or social engineering (using personal details from vacation plans or wedding lists to build trust). For the hospital, the "Shift schedules" could be used to plan physical intrusions or cyberattacks during low-staffing periods, and "Employee budget" could reveal financial weaknesses or targets for corporate espionage. • The information could be used against other employees. "Shift schedules" might reveal names and work patterns of other staff, making them targets for social engineering, phishing, or even physical threats. The "Wedding list" could expose PII of friends and family, making them vulnerable to scams or targeted attacks. • The information could be used against relatives. The

	"Wedding list" explicitly contains names of relatives and friends, making them susceptible to phishing attempts, imposter scams, or other social engineering tactics where an attacker pretends to be Jorge or someone else they know. • The information could provide access to the business. Details from the "New hire letter" or "JB_Resume" could be used to craft convincing phishing emails targeting Jorge to gain network credentials. Knowledge of "Shift schedules" could aid in physical reconnaissance or planning an insider threat operation.
Risk analysis	• To mitigate these types of attacks, technical controls like mandatory encryption for all portable storage devices (USB drives) would prevent unauthorized access to data if the device is lost. Operational controls should include strict policies prohibiting the storage of work-related information on personal devices and vice-versa, coupled with regular employee training on data handling and the dangers of "found" USB drives. Managerial controls involve enforcing these policies with disciplinary actions and regularly auditing compliance to ensure adherence. • Malicious software such as ransomware, keyloggers, or backdoors could be hidden on these devices. If an infected device were discovered and used by another employee, it could lead to a widespread network compromise, data exfiltration, or the encryption of critical hospital systems, severely impacting patient care and operational continuity. • A threat actor could find highly sensitive information on a device like this, including employee PII (names, contact info, employment history), internal hospital operational details (staffing, schedules), and potentially financial data (budgets). • This information might be used against an individual for identity theft, blackmail, or targeted social engineering. Against an organization, it could lead to corporate espionage, network breaches, ransomware attacks, or reputational damage due to leaked sensitive data.