Parking lot USB exercise

Contents	The USB stick contained a mix of work-related and personal files, including employee shift schedules, budget spreadsheets, resumes, new hire letters, and personal media such as family photos and a wedding list. Several of these files contain PII (Personally Identifiable Information) such as names, roles, and possibly salaries or contact details. Yes, some files clearly contain sensitive work information (Shift schedules, Employee budget, New hire letter, JB_Resume). It is not safe to store personal files with work-related files, as this practice increases the risk of data exposure, identity theft, and the blending of professional and personal boundaries.
Attacker mindset	An attacker could use the resume, shift schedules, or budget documents to learn about hospital operations, employee structure, and salary details. This information can be used to target employees with phishing attacks, impersonate HR staff, or build convincing scams. Family-related or personal documents could also help attackers launch spear-phishing attacks on Jorge, his relatives, or colleagues. If malware had been embedded in the USB, it could serve as a backdoor into the hospital's internal network, giving attackers access to broader systems and patient data.
Risk analysis	A malicious USB like this could contain malware such as keyloggers, ransomware, remote access trojans (RATs), or data-stealing scripts. If plugged into a hospital device outside of a secure sandbox or virtual environment, it could lead to network compromise, data theft, or even shutdown of hospital systems. To mitigate this, organizations should apply: Technical controls: Disable auto-run USBs, enforce endpoint protection, and use USB scanning tools. Operational controls: Only analyze unknown USBs in isolated virtual environments or forensic workstations. Managerial controls: Train employees on the risks of USB baiting and create clear policies forbidding connection of unknown devices. Information found on such USBs could be used to manipulate, impersonate, or blackmail individuals, or to gain unauthorized access to hospital IT infrastructure.