Parking lot USB exercise

Contents	The USB drive contains both personal and professional documents, including family and pet photo folders, a resume, and work-related items like employee budgets, shift schedules, and onboarding letters. Many of these files include personally identifiable information (PII), such as names, employment status, and possibly contact details.
Attacker mindset	An attacker could exploit Jorge's resume, staff schedules, and internal HR documents to launch phishing attacks or impersonation schemes targeting employees. If staged, the USB drive might distract users with innocent content while silently installing malware or establishing unauthorized access to hospital networks during a moment of trust.
Risk analysis	Malicious USB devices can contain payloads like keyloggers, ransomware, or remote access trojans. Even without malware, exposed sensitive files give attackers insight into hospital operations, employee routines, and hiring procedures. To mitigate such threats, organizations should implement strict USB policies, mandate sandbox testing environments, and educate staff to never plug in unknown drives. Disabling USB ports on sensitive systems and enforcing encryption on authorized devices adds another layer of protection.