Parking lot USB exercise

Contents	The USB device may contain personal identifiable information (PII) such as names, addresses, or employee data, as well as sensitive hospital-related work files like patient records, schedules, or financial documents. Storing personal files together with work files is unsafe because it increases the risk of exposure, data leakage, and confusion between personal and professional use.
Attacker mindset	If an attacker gains access to this device, they could use the information to impersonate Jorge, launch phishing attacks, or gain access to the hospital's systems. The files could also be leveraged to target other employees through social engineering, or even exploit relatives if personal contact details are exposed. Ultimately, the USB could provide attackers with entry points into the hospital's network or sensitive operations.
Risk analysis	A malicious USB could contain malware such as keyloggers, ransomware, or trojans, which might execute as soon as another employee plugs it in. If infected, the malware could steal sensitive hospital data, disrupt operations, or give attackers remote access. Threat actors could find patient data, internal communications, or login credentials, which can be exploited for identity theft, financial fraud, or blackmail. Technical controls (like disabling autorun, endpoint protection, and USB port restrictions), operational policies (training employees not to use unknown USBs), and managerial controls (clear data handling policies) can reduce these risks.