Parking lot USB exercise

Contents	*The USB drive holds a mix of personal photographs (family and pets) and sensitive work documents, including a new hire letter and an employee shift schedule that contain names, contact details, and employment information. This device clearly contains PII such as dates of birth and home addresses, as well as internal hospital records. Combining personal and corporate files on one device increases the likelihood of accidental data disclosure and complicates incident response.*
Attacker mindset	*An attacker could extract employee PII and HR documents to craft highly convincing spear-phishing or credential-harvesting campaigns targeting Jorge, other staff, or relatives. Social engineering attacks might leverage personal photos to build trust, while the presence of hospital paperwork could trick employees into running malicious executables hidden on the drive, providing the attacker a foothold into the network. Such tactics could facilitate broader compromise or unauthorized access to internal systems.*
Risk analysis	*Malware such as ransomware, Trojans, or keyloggers can be disguised in seemingly benign files and auto-execute when the drive is accessed. If another employee plugged in the device, the malware could spread laterally before detection, encrypting data or stealing credentials. An adversary could also obtain PII to commit identity theft or launch targeted insider threats against the hospital. Implementing technical controls (e.g., disabling USB ports, endpoint security with device whitelisting), operational procedures (e.g., scanning drives in isolated environments), and managerial policies (e.g., strict media acceptance guidelines) reduces USB baiting risks.*