Parking lot USB exercise

Contents	The USB drive contains both personal and work-related files, including family and pet photos, a new hire letter, and an employee shift schedule. These documents may contain personally identifiable information (PII) and sensitive internal data. Storing personal and business files together on an unsecured USB drive is risky and not recommended.
Attacker mindset	An attacker could use the employee schedule to impersonate staff or plan targeted phishing attacks. Personal photos and documents could help in crafting convincing social engineering messages. The presence of HR-related files might provide insight into internal operations, increasing the risk of unauthorized access to hospital systems.
Risk analysis	USB baiting attacks can deliver malware such as ransomware, spyware, or keyloggers that infect systems once the device is plugged in. If an unsuspecting employee had accessed this USB on a networked computer, it could have compromised sensitive data or granted attackers a foothold in the hospital's network. The personal and business information could also be exploited for identity theft or business disruption. To mitigate such risks, organizations should implement USB usage policies, disable USB ports where possible, and educate staff on safe practices like using secure, encrypted storage and analyzing unknown devices in isolated virtual environments.