Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. ● *Are there files that can contain PII?* ● *Are there sensitive work files?* ● *Is it safe to store personal files with work files?* Certain documents contain sensitive personal information that Jorge would prefer to keep private. These files also contain personally identifiable information (PII) belonging to other individuals. Additionally, the work documents contain details about the hospital's operational activities.
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. ● *Could the information be used against other employees?* ● *Could the information be used against relatives?* ● *Could the information provide access to the business?* Timesheets hold information that could give an attacker insights into Jorge's colleagues. This data could include both professional and personal details. The attack could use malicious emails and mimic communication from a coworker or family member.
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: ● *What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?* ● *What sensitive information could a threat actor find on a device like this?* ● *How might that information be used against an individual or an organization?* Increasing employee awareness of USB drive-related attacks, coupled with managerial guidance on response protocols, reduces risks. Implementing a routine of antivirus scans as an operational control can fortify defense against malicious activities.