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?* *They contain his name so that is one piece of PII that is exposed. The device also stores personal photos which could contain PII. He also keeps some work files such as a new hire letter, budget, and shift schedules.*
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?* *They can frame Jorge as they have his personal files and work files and make it seem like he is an attacker. They can steal his identity and possibly gain access to sensitive data using his credentials.*
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?* *Someone could have added malicious code to the USB or files that would lead to a backdoor or trojan horse as some people may call it. The device could lead to a hack of a system that previously wasn't vulnerable.*