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?* *The given document has personal and work files related. Jorge also has a USB containing information for a new hire and therefore PII information. Furthermore, an individual should not store personal files with work files as we need to lower authorization and access.*
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?* *Unfortunately, this means that information can be exploited by hackers. Because the information has PII, it can be used against other employees and gather information that can be used against them. The hacker could pretend to be someone or have information on a mutual individual and trick Jorge or other employees to give away private information.*
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?* *Employees should be trained and aware of these type of attacks that can be taken against them. The company should be aware of suspicious activity and files that can reduce the impact. A type of technical controls the business can implement is MFA , AAA and operational methods such as audits to regularly check up on logs, and even managerial controls such as creating policies and ensuring that all employees follow up reducing human error and improving security awareness.*