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?*
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?*
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?*

Contents: There are files that contain PII including his resume and information about his wedding and who he's inviting. There are also pictures of him and his family. As for sensitive work files, yes, shift schedules and the employee budget. No it is not safe to store personal files with work files. It makes it more difficult to have proper separation between work and personal life.
Attacker mindset: The information could be used against other employees or against HR if someone is looking for either less or more hours and sees someone else's schedule is more ideal than theirs. Against relatives, well the family photos and dogs pics could be used maliciously against the members that are in the pictures. Depending on the contents of the work-related documents, it is possible the info could provide access to the business

Risk Analysis: The USB could contain viruses such as one where it autoruns and copies all files of the computer it is plugged into. It could also deploy some spyware or keylogging services which could provide the threat actor with login credentials. The USB could also contain banking information or records, or a password file, or SPII such as copies of a birth certificate, health card, driver's license, credit card into, health records etc. If there is SPII, then identity theft and financial fraud could easily happen if exposed. Also, if any records pertain to the organization, it could also cause damage to the company, depending on the info found. E.g. if there's company credit card info, then instant financial damage if used by a threat actor. If there are confidential product files or business strategy files, then if a competitor or activist gets their hands on it, they would either use it to take money or clients from the company or use it to effectively sabotage the plans of the company.