Parking lot USB exercise

Problem Statement

You've discovered a USB drive in a parking lot. Upon analysis, it is found to belong to an employee of a hospital and contains a mix of personal and confidential work-related files. Your task is to analyze the contents, adopt an attacker's mindset to understand the potential risks, and recommend a strategy to mitigate **USB baiting attacks**, a type of social engineering attack where a threat actor leaves a USB drive in a public place, hoping a victim will plug it into a machine.

Contents	The USB drive contains a mix of personal and work related files, including family and pet photos, a new hire letter, and an employee shift schedule. This suggests that Jorge may have used the device for both personal and professional purposes, potentially storing sensitive personally identifiable information (PII) and confidential work related data. The device may pose a security risk if it falls into the wrong hands.
Attacker mindset	An attacker could use the information on the USB drive to target Jorge or the hospital by exploiting the sensitive personally identifiable information (PII) and confidential work related data. The attacker might use this information to conduct phishing attacks, steal identities, or gain unauthorized access to the hospital's systems. This could potentially lead to data breaches or other malicious activities.
Risk analysis	To mitigate USB baiting attacks, technical controls such as endpoint security software and intrusion detection systems can help identify and block malicious code. Operational controls like USB port blocking and strict device usage policies can also reduce the risk. Managerial controls, including employee education and awareness training, can help prevent employees from plugging in unknown devices. Implementing a combination of these controls can effectively mitigate the risks associated with USB baiting attacks.