Parking lot USB exercise

Contents	*The USB stick appears to belong to an employee of the hospital, because it contains documents relating to the job, like a resume, employee budget, and a shift schedule. However, it also contains personal documents relating to a wedding and a vacation, which are likely to contain personally identifiable information (PII).*
Attacker mindset	*There are a few ways an attacker could use the information against the employee or the entire organization. For instance, he could use the personal data to target the employee, his family, or his closest friends. Additionally, he could use what he gathers from the business documents to compromise normal operations and steal sensitive information. Or, he could use steganography to embed malicious code into any one of those files and execute it once the USB stick is inserted into the network.*
Risk analysis	*Sandboxing and virtualization are effective ways to deal with USB baiting, because it allows for analysis of a USB stick for potential malware without having it affect the main network. Also, as a general rule, it is wise not to mix personal and business files on any device, especially if it is corporate-owned.*