Parking lot USB exercise

Contents	Upon inspection of the found USB drive using the virtualization software, we discover several types of files. Some of which are work-related and could contain Personally Identifiable Information (PII) such as names, addresses, and other sensitive information. Additionally, the USB includes personal files. Combining personal files with work files on the same device is not safe practice as it may expose personal information to malicious actors and complicate data management and protection strategies.
Attacker mindset	Given the types of information found, a malicious actor could potentially use the data in a number of ways. The PII from patient records could be used for identity theft or even blackmail purposes. The work files could provide insights into hospital operations, potentially allowing unauthorized access to hospital systems or even physical areas within the hospital. Even the personal files could provide social engineering fodder, giving an attacker the means to impersonate or manipulate hospital staff or their relatives.
Risk analysis	*There are several technical, operational, and managerial controls that could help mitigate such risks. Technically, antivirus software and intrusion detection systems could identify and quarantine malicious software hidden on devices. Operationally, policies could be put in place requiring the use of encrypted USB drives for transporting data, regular training of staff on data security practices, and procedures for handling found devices. Managerially, a clear separation of work and personal files should be enforced, as well as stringent access controls and auditing on sensitive data. Additionally, lost and found protocol should be established, ensuring that misplaced devices are returned to the IT department for proper handling. If the device was infected and discovered by another employee, without these protocols, it could have been plugged into the hospital's network, potentially causing a system-wide infection or data breach.*