# Parking lot USB exercise

| | |
|---|---|
| **Contents** | Write **2-3 sentences** about the types of information found on this device.<br>● *The USB contains both personal and work-related files. Personal items include family and pet photos, which are considered personally identifiable information (PII).*<br>● *Work files include employee shift schedules and a new hire letter.*<br>● *Storing sensitive personal data alongside hospital documents increases the risk of exposure if the drive is compromised.* |
| **Attacker mindset** | Write **2-3 sentences** about how this information could be used against Jorge or the hospital.<br>● *An attacker could exploit Jorge's personal data for phishing or social engineering, targeting him or his relatives.*<br>● *Work-related files such as employee shift schedules could help plan physical or insider attacks on the hospital.*<br>● *The attacker might also copy the USB, embed malicious code, and re-drop it to infect hospital systems with malware or ransomware.* |
| **Risk analysis** | Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks:<br>● *To reduce USB baiting risks, technical controls like disabling USB autorun and enforcing endpoint protection should be applied.*<br>● *Operationally, employees must be trained to avoid inserting unknown devices and instead report them immediately to security staff.*<br>● *Managerial controls include establishing clear data handling policies and separating personal and work storage. Regular cybersecurity awareness campaigns will strengthen vigilance, while sandbox or virtual* |

| | |
|---|---|
| | *environments can be used for safe examination of suspicious USB drives.* |