## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | The USB drive contains several documents, including spreadsheets with patient names and appointment schedules, which could contain personally identifiable information (PII). There are also files labeled as internal reports and policy drafts, suggesting sensitive work files are present. It is unsafe to store personal files alongside work files, especially on portable devices, as this increases the risk of accidental data leaks or exposure to malware. |
| **Attacker mindset** | An attacker could use the information found on the USB to impersonate hospital staff, launch phishing attacks, or gain deeper access into the hospital’s network. Details like staff names, schedules, or internal documents could be used to socially engineer other employees or even patients. If login credentials or operational procedures are stored on the USB, it could lead to a breach of confidential systems or patient records. |
| **Risk analysis** | This USB could potentially contain malware such as keyloggers, ransomware, or trojans designed to extract data or grant remote access to the attacker. If a curious employee had plugged it into a network-connected device, it might have compromised hospital systems or leaked sensitive data. Threat actors could exploit information like patient data or employee contacts for identity theft, blackmail, or targeted cyberattacks. To mitigate these risks, organizations should enforce policies for handling unknown devices, use virtualization or sandbox environments for inspection, provide regular employee training on social engineering, and implement endpoint protection solutions that can detect unauthorized USB activity. |