Identify the attack vectors of a USB drive

Scenario

Review the following scenario. Then assess the attack vectors of a USB drive.

You are part of the security team at Rhetorical Hospital and arrive at work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. No one else might have dropped it, so you decide to pick it up out of curiosity.

You bring the USB drive back to your office where the team has virtualization software installed on a workstation. Virtualization software can be used for this very purpose because it's one of the only ways to safely investigate an unfamiliar USB stick. The software works by running a simulated instance of the computer on the same workstation. This simulation isn't connected to other files or networks, so the USB drive can't affect other systems if it happens to be infected with malicious software.

Contents	The USB drive contains personal and work-related files, including family and pet photos, a new hire letter, and an employee shift schedule.
Attacker mindset	The attacker could use the personal information to blackmail Jorge or his family or to target them for identity theft. They could also use the work-related information to launch a phishing attack against the hospital or gain access to its systems.
Risk analysis	The hospital should implement policies and procedures to prevent employees from storing personal information on work-related devices. They should also use virtualization software to scan all USB drives before they are plugged into any workstations.