Parking lot USB

Scenario

You are part of the security team at Rhetorical Hospital and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. There's no one else around who 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 stick was found to contain several sensitive files. These included spreadsheets with patient names, medical record numbers, and treatment history — all classified as **Personally Identifiable Information** (**PII**) and **Protected Health Information** (**PHI**). Personal files (e.g., photos or resumes) with work documents were also noted, increasing the risk of unauthorized data exposure and potential cross-contamination between personal and professional content.
Attacker mindset	An attacker could exploit the data to target hospital staff or patients. For example, they might use PII for **phishing attacks**, impersonate hospital staff to gain access to internal systems, or even leak PHI for financial or reputational damage. The presence of hospital branding on the drive also adds a layer of **social engineering** credibility, making it easier to trick employees into plugging it in. Family members of patients could also be targeted if their information was present in related files.

Risk analysis	To reduce the risk of infected USB drives, unknown USB devices should only be analyzed in isolated virtual environments and sandboxed only. Staff should be trained not to plug in unfamiliar devices and report them instead. Security settings should block USB auto-run and limit access to only approved, scanned devices. Establish data classification policies and enforce secure storage practices for sensitive files.