# **1. Data-Flow sketch**

# **2. Risk analisys**

**1) Destination-country laws/practices (USA)**

**Risk R1 — Government access during a support session.**  
**Reasoning:** Under *Schrems II*, exporters must assess whether third-country law undermines SCC guarantees. Certain U.S. surveillance powers may allow access that is not “essentially equivalent” to EU standards. During a break-glass window, the importer can view health data in real time.  
**Why relevant:** The sub-processor is under U.S. jurisdiction; access, though read-only, concerns highly sensitive personal data.  
**Likelihood:** **Low** (sessions are rare, authorised, and time-boxed).  
**Impact:** **Very high** (special-category data; potential duty to suspend the transfer if SCCs cannot be honoured in practice).

**Risk R2 — “Gag orders” blocking notification and undermining SCC compliance.**  
**Reasoning:** The 2021 SCCs require the importer to notify the exporter of government access requests and to stop processing if compliance is impossible. U.S. secrecy orders may prohibit such notification.  
**Why relevant:** Directly affects the ability to apply protections and to suspend the transfer promptly.  
**Likelihood:** **Very low – Low**.  
**Impact:** **High – Very high** (may require immediate suspension; legal and operational disruption).

**2) Nature of data (special category: health)**

**Risk R3 — Special-category health data with potentially broad scope.**  
**Reasoning:** DICOM images and clinical identifiers are special-category data under GDPR, highly sensitive and may involve multiple studies or series. Even limited exposure can meaningfully affect data subjects.  
**Why relevant:** Metadata such as MRN and accession numbers are identifiers  
**Likelihood:** **Constant** (inherent to the processing).  
**Impact:** **Very high** (reputational harm, discrimination risk, regulatory consequences).

**3) Attacker model (technical/organizational threats)**

**Risk R4 — Unintentional exfiltration during the session (downloads, log export, screenshot).**  
**Reasoning:** Support tools or logs can create unintended copies outside the intended perimeter.  
**Why relevant:** DICOM and logs carry identifiers; any extra copy outside the intended perimeter can be dangerous.  
**Likelihood:** **Low** (read-only, auditing, encryption)  
**Impact:** **High** (personal-data breach).

**Risk R5 — Insider misuse at the U.S. sub-processor.**  
**Reasoning:** Privileged users might access more than necessary within the time-boxed window.  
**Why relevant:** Even short temporary access rights may allow exposure of multiple records.  
**Likelihood:** **Low** (role-based access, MFA, dual approval, session recording).  
**Impact:** **High** (rapid exposure of multiple records).

**Risk R6 — Interception of the support channel (MITM).**  
**Reasoning:** Cross-border remote access requires strong transport security; weaknesses could expose data in transit.  
**Why relevant:** Real-time traffic between U.S. endpoints and EU systems.  
**Likelihood:** **Very low** (with robust VPN + TLS and IP allow-listing).  
**Impact:** **Medium–High** (exposure of content/credentials).

**Risk R7 — Misconfiguration expanding scope (read-only → write/export).**  
**Reasoning:** Errors in configuration or permissions could disable safeguards and enable data modification or export.  
**Why relevant:** The case specifies that the sub-processor’s access is **read-only** and requires approval; if these restrictions are not correctly applied, exposure risk increases.  
**Likelihood:** **Low** (depends on the rigour of configuration controls).  
**Impact:** **Very** **high** (loss of control; larger attack surface).

**Risk R8 — Re-identification via operational metadata/artifacts (logs, MRN, Ips, accession).**  
**Reasoning:** Technical data can still identify or link individuals through correlation.  
**Why relevant:** Logs are part of the processing and may be visible during support.  
**Likelihood:** **Medium** (logs are often verbose).  
**Impact:** **Medium–High** (expands the personal-data footprint; correlation risks).

# **3. Transfer Tool & safeguards**

# **4. Conclusion & accountability**