



id: SI_006

model: anthropic/claude-sonnet-4.6

seeds:

04_risiko: sårbarhet

03_relasjon: makt

05_handling: utforsk

01_perspektiv: strategisk

02_tidhorisont: kortsiktig

Instans SI_006

Seeds: strategisk | kortsiktig | makt | sårbarhet | utforsk

Maktanalysen ingen nevner: Hvem eier svermen?

Den strategisk kritiske fellen i helsevesen-kontekst: **Copilot Studio gir Microsoft makt over din orkestreringslogikk.** Du bygger på en plattform der Microsoft kan endre prising, API-grenser og compliance-krav over natten. For en 200-ansatt helseorganisasjon med strenge dataregimer er dette en **strukturell sårbarhet** — ikke et hypotetisk scenario.

Anbefalt arkitektur: Azure OpenAI + Durable Functions som orkestrator

```
# Pseudo-orkestrering: Durable Functions fan-out
@app.orchestration_trigger
def swarm_orchestrator(context):
    specialist_configs = load_agent_roles("SharePoint:/agent_registry.json")
    # Parallell fan-out – 100 agenter
    tasks = [context.call_activity("run_agent",
                                   {"role": cfg["role"],
                                    "system_prompt": cfg["prompt"],
                                    "case_context": inject_from_dataverse(case_id)})
              for cfg in specialist_configs]
    results = yield context.task_all(tasks)
    return synthesizer_agent(results)
```

Dette **beholder Microsoft-investering** (Azure, Entra ID, Dataverse) men gir deg orkestreringslogikk du eier.



Sårbarhetspunkt du må adressere nå

- **Data residency:** Azure OpenAI i Norway East støtter PHI — **krev dette eksplisitt i deployment**, ikke default
- **Agent-differensiering:** 100 identiske prompts er ubrukelig. Bygg en `agent_registry` i SharePoint/Dataverse med unike `system_prompt` + `retrieval_scope` per rolle. Regulatory reviewer får kun lovtekst-embeddings; cost-analyser får kun Dataverse-budsjetttabeller
- **Consistency i Case 2:** Bruk `temperature=0` + structured output (JSON schema enforcement) per agent. Variabel case-kompleksitet løses med **routing-agent** som pre-klassifiserer og tildeler ressursnivå

Kortsiktige quick wins (0-8 uker)

Ikke start med 100 agenter. Start med **3-agent fan-out** på ett reelt problem — f.eks. innkjøpsanalyse. Bevis ROI internt før governance-prosessen stenger deg ute.

Konkrete neste steg

1. **Uke 1-2:** Kartlegg hvilke data som aldri forlater tenant — definer hard boundary for agent context injection via Azure AI Search over intern indeks
2. **Uke 3-4:** Deploy minimal Durable Functions-orkestrator med 3 differensierte agenter på én reell case-type
3. **Uke 5-8:** Implementer Application Insights token-tracking per agent-rolle — dette blir ditt kostnads- og compliance-argument for videre skalering