

# RISIKO OG MULIGHETER VED IMPLEMENTERING AV IT-SYSTEMER

---

ANDERS BERGMAN

IT-BEDÖMMER FOR NORSK AKKREDITERING OCH SWEDAC

# HVILKE KRAV OPPFYLLER IKKE SÅ MANGE?

---

- Tjensteavtaler med IT-tjensteleverantører inom HF/RHF
- Avvikshantering av IT-incidenter/hendelser
- Managring av mellomprogramvare
- Validering av integrasjoner ved oppgradering av Journalsystemer i primærhelsetjensten
- Internrevisjoner av IT-tjensteleverantør(-er)
- Oppfølging av tjensteleveranser från IT-tjensteleverantører
- Informasjonssikkerhet i paritet med nationella/RHF/HF-krav
- Risikoanalyser ved införande av nya systemer och större ändringar
- Samtlige lovkrav enligt Pasientdataloven
- Meddela større tekniska förändringar till NA i god tid innan planerat införande
- Egenutvikling av IT-systemer

# TING BLIR BEDRE OG BEDRE... 😊

---

- Tjensteavtaler med IT-tjensteleverantører inom HF/RHF
- Avvikshantering av IT-incidenter/hendelser
- Managring av mellomprogramvare
- Validering av integrasjoner ved oppgradering av Journalsystemer i primærhelsetjensten
- Internrevisjoner av IT-tjensteleverantør(-er)
- Uppfølging av tjensteleveranser från IT-tjensteleverantörer
- Informasjonssikkerhet i paritet med nationella/RHF/HF-krav
- Risikoanalyser ved införande av nya systemer och större ändringar
- Samtlige lovkrav enligt Pasientdataloven
- Meddela større tekniske förändringar till NA i god tid innan planerat införande
- Egenutvikling av IT-systemer

# IT-ORGANISASJON

---



# ANSVAR

---

- IT innen HF er ansvarlig for styring og fungerer noen ganger som bestiller for IT-drift
- IT-drift er ansvarlig for levering av nettverk og operasjonelle tjenester innenfor signerte SLA-avtaler, og noen ganger også for applikasjonsstøtte.
- IT-leverandøren er ansvarlig for å tilby support i henhold til en signert avtale
- Virksomheten er ansvarlig for kvaliteten på informasjonen, dvs. informatikk og informasjonssikkerhet
- Den akkrediterte virksomheten er ansvarlig for kvaliteten på informasjon (informatikk og informasjonssikkerhet), og for å overvåke at ovennevnte tjenester leveres i tide og med forventet kvalitet

# REVISJON/OPPFÖLGING

---

- Avtaler med leverandører av IT-drift bør følges opp en gang i kvartalet
- Avtaler med applikasjonsleverandører skal følges opp minst en gang i året
- HF's overordnede regler innen IT bør følges opp minst to ganger i året

# INFORMASJONSSIKKERHET

---

- Normen - Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten
- Regler for informasjonssikkerhet innen HF, regler
- GDPR, lov med overtredelsesgebyr
- Bruk ISO / IEC 27000-serien som rammeverk ..



# INTEGRASJONER

---

- Mellom systemer/funksjoner i den akkrediterte virksomheten, for eksempel labinstrumenter, mellomprogramvarer og andre labsystemer.
- Mellom systemer/funksjoner i Sykehus/HF, for eksempel EPJ
- Mellom systemer/funksjoner nasjonalt, for eksempel EPJ i legekontor og nasjonale tjenester og kjernesjournal
- Generelt prinsipp: Den akkrediterte virksomheten er alltid ansvarlig for kvaliteten på informasjonen i integrasjoner, dvs. fra bestilling i kundens system til presentasjon av prøvesvar i kundens system. Noen unntak finnes imidlertid, ex. svarrapportering via det norske helsenetet.



# ”DIGITALISERING”

---

- Digitalisering - en fantastisk mulighet for effektivitet og økt samhandling med pasienter og innbyggere
- Men.... høy risiko for at det ikke tas tilstrekkelig med hensyn til informasjonssikkerhet når hastigheten er høy og samfunnets krav er store

# ENDRINGSLEDELSE

---

- GDPR - Privacy by design, må tas i betraktning når du beholder større systemendringer så vel som systemendringer
- Datatilsynet: *Innebygd personvern* er et sentralt krav i personopplysningsloven og betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Dette skal sørge for at informasjonssystemene oppfyller personvernprinsippene, og at de ivaretar de registrertes rettigheter.
- Viktig å ta hensyn til kravene i GDPR Art 35 – Vurdering av personvernkonsekvenser og forhåndsdrøftelse (DPIA)
- Datatilsynet: Sjekkliste for vurdering av personvernkonsekvenser (pdf)

# TAKK FOR OPPMERKSOMHETEN....

---

- Noen spørsmål?