IMY. Integritetsskydds myndigheten

LÄKEMEDELSVERKET
SWEDISH MEDICAL PRODUCTS AGENCY

Säker AI-användning i vården

Utifrån MDR/IVDR och GDPR

Webbinarium: 21 oktober 2026

Webbinariet är en del av årets Tänk säkert-kampanj

- Oktober är den årliga informationssäkerhetsmånaden.
- Syftet är att öka medvetenheten om informations- och cybersäkerhet
- I år genomför IMY och Läkemedelsverket det här webbinariet tillsammans som en del av kampanjen.

IMY. Integritetsskydds myndigheten

LÄKEMEDELSVERKET
SWEDISH MEDICAL PRODUCTS AGENCY



Agenda

- Ett exempel på AI i vården
- Introduktion av våra roller och regelverk
- Vad innebär regelverken i praktiken?
- Risker och mänsklig översyn
- Uppföljning
- Våra medskick
- Frågestund
- Lästips

Exempel på AI i vården

SCENARIO · EN VANLIG MOTTAGNING

Läkaren trycker på ”Spela in”



Patienten har skadat höger fot. Mötet börjar – och AI-tjänsten startas.

SCENARIO · EN VANLIG MOTTAGNING

Samtalet spelas in



Medan vi pratar skapas en ljudfil – med röster och hälsouppgifter.

1 Spela in | **2 Ljudfil** | 3 Transkript | 4 Journalutkast

SCENARIO · EN VANLIG MOTTAGNING

Tal blir text – rådata

TRANSKRIPT · ORDAGRANT, UTAN TALARE MARKERADE

Hej! Jag förstår att du har skadat höger fot. Kan du berätta vad som hände? Ja, jag spelade fotboll igår och landade snett. Foten vek sig inåt och jag kände direkt att det gjorde jätteont. Okej. Var det en tydlig vridning inåt, alltså ett så kallat inversionsvåld? Ja, precis. Den vek sig inåt. Hörde du något ljud, som ett knäpp? Ja, det kändes nästan som ett knäpp eller en smäll. Kunde du belasta foten direkt efter skadan? Nej, jag fick halta av planen. Hur snabbt kom svullnaden? Inom några minuter. Den blev stor direkt. Har du haft liknande skador tidigare? Jag stukade foten för några år sedan, men inte så här illa. Har du gjort någon egen behandling? Jag har haft den i högläge och kylt lite. Bra. Har du domningar, stickningar eller känselbortfall? Nej, inget sånt. Då ska jag undersöka foten. Säg till om något gör ont.

Språkmodellen skriver ett journalutkast

Transkript

Prompt och instruktioner

Journalmall

↓

Språkmodell
ofta en GPAI-modell

→

JOURNALUTKAST · ATT GRANSKA OCH SIGNERA

Besöksorsak
Högersidig fotledsskada

Aktuellt
Snedlandning vid fotboll i våras med inversionsvåld mot höger fot, omedelbar kraftig smärta, upplevelse av knäpp/smäll, snabb och uttalad svullnad, initialt svårt att belasta och fick halta av planen. Kan nu gå kortare sträckor men hoppar och avlastar lateralt. Tidigare fotstukning för några år sedan, lindrigare. Egenbehandlat med högläge. Förnekar domningar, parestesier, känselbortfall.

Tidigare sjukdomar
Tidigare fotstukning för några år sedan.

Status · Allmäntillstånd
Avlastar lateralt vid gång.

Lokalstatus
…

SCENARIO · VAD SÄGER TRANSKRIPTET?

Titta en gång till

Patienten sa	Journalutkastet skriver	Vad hände?
”Jag spelade fotboll igår”	”… vid fotboll i våras …”	**Förvrängning**
– (sades aldrig)	”Kan nu gå kortare sträckor men hoppar och avlastar lateralt”	**Tillägg**
– (undersökningen spelades inte in)	Status: ”Avlastar lateralt vid gång.”	**Tillägg**
”Jag har haft den i högläge och kylt lite”	”Egenbehandlat med högläge.”	**Utelämnande**

Det ser proffsigt ut – och det är just därför det är svårt att upptäcka.

Introduktion av våra roller och regelverk



IMY och Läkemedelsverket tillsammans

- Komplext när olika regelverk behöver samverka.
- Produkter och tjänster integreras i vårdprocesser och där hälsodata behandlas för att uppnå sitt syfte.
- Regelverken är hanterbara – och kan vara möjliggörare.
- GDPR och MDR har gemensamma beröringspunkter – och AI-förordningen läggs ovanpå.
- Därför gör IMY och Läkemedelsverket det här tillsammans.

Läkemedelsverkets roll

- Tillsyn över medicintekniska produkter och deras tillverkare
- Marknadskontrollmyndighet enligt MDR – och enligt AI-förordningen när AI-systemet är en medicinteknisk produkt
- Säkerhetsövervakning: vi tar emot tillverkar- och vårdrapporter om negativa händelser
- Främja innovation för säkra, ändamålsenliga produkter där nyttan överväger risken

Integritetskyddsmyndighetens roll

- Sveriges dataskyddsmyndighet
- Kontrollerar att företag och myndigheter följer dataskyddsförordningen, GDPR
- Vägledning till de som behandlar personuppgifter,
- Främja innovation där rättigheter och effektivitet står i balans
- Ta emot personuppgiftsincidenter

2026: tillsyn och vägledning av AI-transkribering i vården – dagens genomgående exempel



Dataskyddsförordningen (GDPR)

- Dataskyddsförordningen gäller för behandling av personuppgifter. Med personuppgifter menas varje upplysning som rör en identifierad eller identifierbar fysisk person.

- Ett av syftena med dataskyddsförordningen är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

- Dataskyddsförordningen gäller för helt automatiserad behandling, delvis automatiserad behandling och i vissa fall helt manuell behandling av personuppgifter.



MDR och IVDR

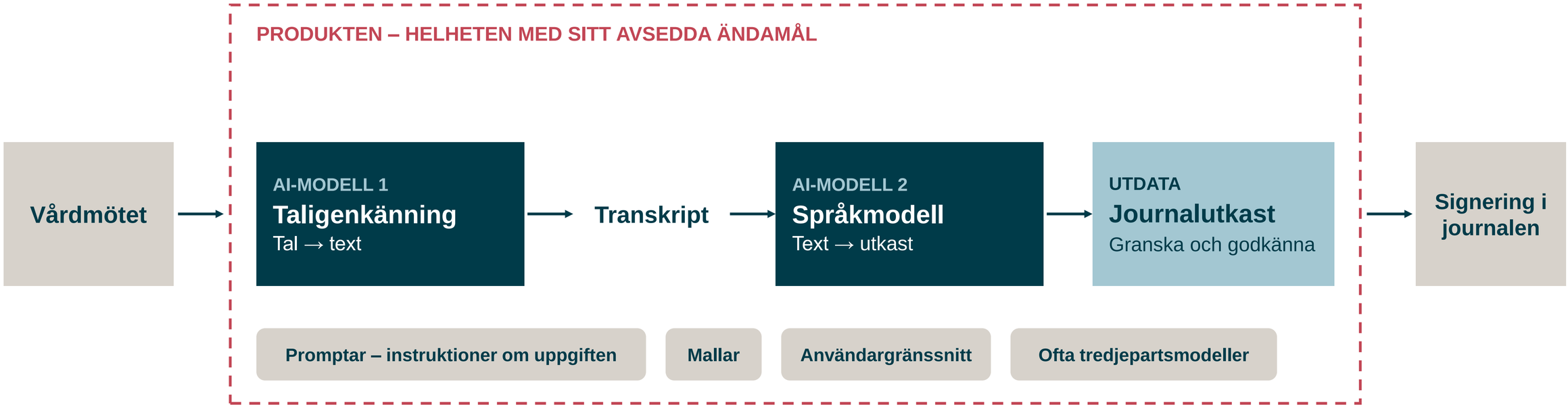
- Programvara är en medicinteknisk produkt när den enligt tillverkaren är avsedd att användas för ett medicinskt ändamål – t.ex. diagnos, övervakning, prediktion eller behandling, eller kompensation av funktionsnedsättning med digitala verktyg (art. 2.1).

- Tillverkaren ansvarar för att säkerställa att produkterna är säkra och fungerar som avsett, och att nyttan överväger riskerna – före och efter CE-märkningen.

- Medicintekniska produkter delas in i klasser utifrån risk och högre klasser måste granskas av tredje part (anmält organ). Det gäller exempelvis programvara som tillhandahåller information för beslut om diagnos eller behandling.

Vad innebär regelverken i praktiken?

Vad är produkten – vad är det som CE-märks och var sker behandling av personuppgifter?



Modellen är inte produkten. Det är helheten som CE-märks och helheten som behöver bedömas.



Hur används systemet i verksamheten?

- Inom vilka användningsområden?
- Anpassas systemet utifrån område?
- Påverkas systemets prestanda?



Ansvar som tillverkare/biträde och personuppgiftsansvarig

- Det är alltid den personuppgiftsansvariga som ansvarar för hur och varför personuppgifter behandlas.
  - Detta inkluderar lämpliga tekniska och organisatoriska åtgärder.

- Personuppgiftsbiträdet ska agera på den personuppgiftsansvarigas instruktioner.

- Tillverkaren ska säkerställa att en medicinteknisk produkt konstrueras och utformas utifrån det avsedda ändamålet – innan den släpps ut på marknaden (MDR).

Ansvar innan och vid behandling av personuppgifter

Innan man börjar behandla personuppgifter

GDPR

När man behandlar personuppgifter

Inbyggt dataskydd och dataskydd som standard

Bedöma riskerna och vidta lämpliga tekniska och organisatoriska åtgärder.

Konsekvensbedömning

Om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

Förhandssamråd

Den personuppgiftsansvariga ska samråda med tillsynsmyndigheten före behandling om en konsekvensbedömning visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvariga vidtar åtgärder för att minska risken.

Säkerhet i samband med behandlingen

- Bedöma riskerna och vidta lämpliga tekniska och organisatoriska åtgärder
- Fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft
- Regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder

Inbyggt dataskydd och dataskydd som standard

- Tekniska och organisatoriska åtgärder ska utgå från
  - den senaste utvecklingen,
  - genomförandekostnader
  - och behandlingens art, omfattning, sammanhang och ändamål
  - samt riskerna, för fysiska personers rättigheter och friheter
  - både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen
- Endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Detta inkluderar
  - mängden insamlade personuppgifter, behandlingens omfattning,
  - tiden för deras lagring och deras tillgänglighet.
  - Inte görs tillgängliga för ett obegränsat antal fysiska personer.

Ansvar före och efter att produkten når vården

Före utsläppande på marknaden

CE

Efter – När produkten används

Tillverkaren – MDR

Konstruktion efter avsett ändamål, riskhantering, validering och klinisk utvärdering

Anmält organ

Granskar kvalitetssystem och teknisk dokumentation – från klass IIa

Tillverkaren – MDR

Klinisk uppföljning efter marknaden, rapportering av allvarliga händelser, hantering av ändringar, övervaka produkten i bruk.

Vårdgivaren – HSLF-FS 2021:52

Rätt produkt, säker användning, rutiner, kompetens och rapportering

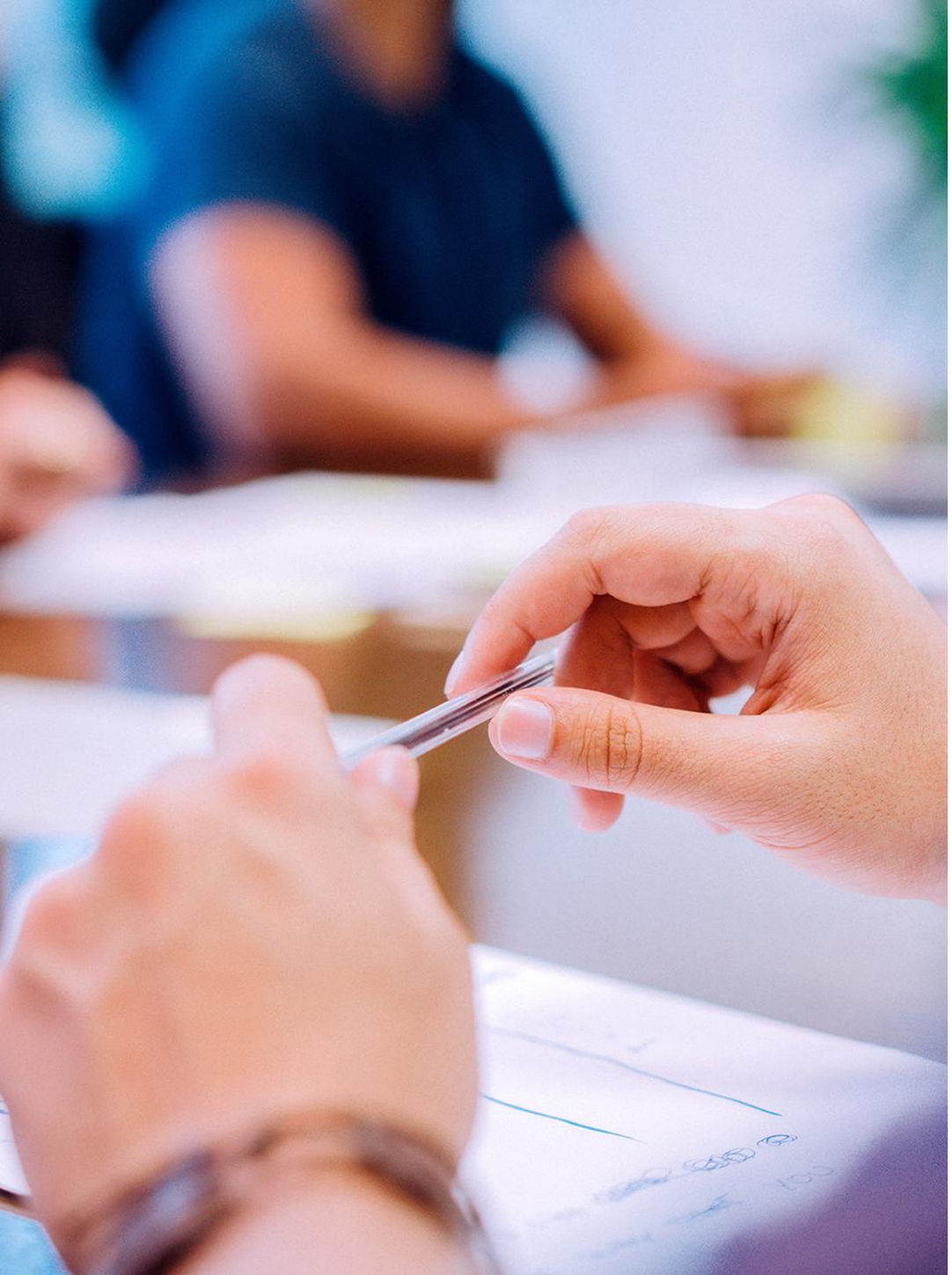
Säkerhet inbyggd från start – MDR bilaga I

Tillverkaren ska

- Hantera risker under hela livscykeln
- Utveckla programvaran enligt en kontrollerad livscykel, med verifiering och validering (17.2)
- Skydda mot obehörig åtkomst och hantera IT-säkerhet (17.2, 17.4)
- Ange minimikrav på hårdvara, nätverk och IT-säkerhet (17.4)

Vårdgivaren behöver

- Uppfylla tillverkarens minimikrav på IT-miljön
- Koppla ihop dem med de egna tekniska och organisatoriska åtgärderna enligt GDPR
- Fråga efter dokumentationen vid upphandling



Validera funktionen – före och under användning

Uppfyller produkten verksamhetens krav?

- Prestanda och klinisk nytta för det avsedda ändamålet
- Verifiering och validering av hela systemet – inte bara modellen

Är lösningen lämplig för vår verksamhet?

- Fungerar den för våra patienter, vår miljö och vårt språk?
- Testa med egna, kända testfall – jämför med facit

Risker och mänsklig översyn



Fånga upp generella risker med AI-baserade system

- Var sker behandlingen?
- Hur säkerställa att data inte förvanskas eller förändras och eventuella ändringar inte fångas upp?
- Process när något går fel.
- Säkerställs det att resultaten som modellen genererar är förväntade samt hur modellens resultat verifieras?
- Används modellen inom olika områden och sker det några anpassningar?
- Hur bevaras systemets integritet och prestanda över tid?
- Ges användaren rätt förutsättningar, inkl. utbildning?

Testa och utvärdera löpande



Andra risker

- **Säkerställa kontinuitet**
  - Vad händer om leverantören går i konkurs?
  - Om modellen driftas i tredjeland som inte kan säkerställa lämplig säkerhet
  - Om modellen stängs ner för vår region
- **Säkerställa att endast behöriga kan ta del av informationen**
  - Är informationen krypterad?
  - Har organisationen kontroll på krypteringsnycklarna?
  - Har endast de som absolut behöver det tillgång till uppgifterna?
- **Ha beredskap för konsekvenser**
  - Viktigt att hålla sig uppdaterad samt vara medveten om (och ha beredskap för) eventuella konsekvenser

Risker med AI-transkribering

01

Tillägg

Innehåll som aldrig sades läggs till

02

Utelämnanden

Viktig information faller bort

03

Förvrängning

Innebörden ändras – t.ex. negationer

04

Automations-bias

Utkastet granskas mindre kritiskt än eget arbete

05

Förändring

Nya modellversioner kan ändra resultatet

06

Spårbarhet

Hur har modellen tagit sina beslut

- **Rapportera: negativa händelser och tillbud ska rapporteras till tillverkaren – och till Läkemedelsverket.**
- **Personuppgiftsincidenter rapporteras till IMY**

Riskerna är inte sällsynta fel – de är förväntade egenskaper hos generativ AI och måste hanteras både i produkten och i användningen.



Meningsfull mänsklig översyn och granskning

- Hur presenteras resultatet?
  - Förstår personen det som presenteras och utifrån det kan ta ett objektivt beslut?
- Får användaren något stöd att tolka resultat?
  - Ex. markerar modellen där den är osäker eller om det är låg tillförlitlighetsnivå på utdatan.
- Finns spårbarhet om något skulle gå fel?
  - Kan man spåra hur modellen har tagit sina beslut och på vilka grunder?
- Finns inbyggda funktioner för att förebygga mänskliga fel?
  - Ex. rimlighetskontroller och spärrar



Signering sänker inte risken

- Kognitiv bias är väl dokumenterat – och en förutsägbar del av användningen
- Granskning och signering är inte skäl för en lägre riskklass
- Mänsklig översyn måste byggas in i produkten: tydlig presentation, markerad osäkerhet och spårbarhet till källan
- Vårdgivaren ger tid, utbildning och rutiner för granskningen

Uppföljning – när produkten förändras

Tillverkaren

- Följer upp prestandan systematiskt efter marknaden
- Bedömer varje ändring – nya modeller, promptar eller mallar – mot det avsedda ändamålet
- En väsentlig ändring kan kräva ny bedömning av anmält organ

Vårdgivaren

- Vet vilken version som används – och när den ändras
- Följer upp kvaliteten i journalerna över tid
- Rapporterar avvikelser till tillverkaren och Läkemedelsverket

Personuppgiftsansvarig

- Följer upp prestandan systematiskt
- Bedömer ändringar – nya modeller, promptar eller mallar – mot det avsedda ändamålet
- Har de vidtagna åtgärderna önskad effekt för att mittigera riskerna
  - Följer upp kvaliteten över tid
  - Krävs förnyad konsekvensbedömning?

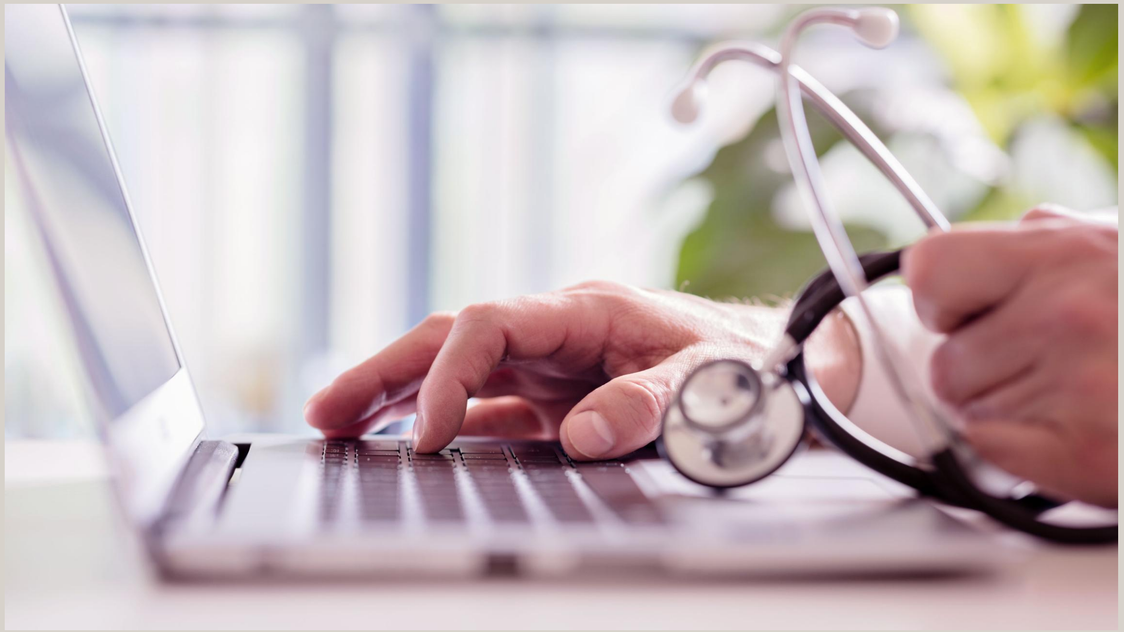
Våra medskick

Sju frågor före upphandling och införande

- Vad gör tjänsten – återger den eller tolkar den?
- Är den CE-märkt – för just vår användning?
- Är prestandan visad för våra patienter och vår miljö?
- Vem är tillverkare – och vem svarar för tredjepartsmodellerna?
- Uppfyller vår IT-miljö tillverkarens minimikrav?
- Hur hanteras uppdateringar och nya modellversioner?
- Regulatoriskt stöd kan efterfrågas av Läkemedelverket

Några viktiga punkter innan personuppgiftsbehandlingen påbörjas

- Bedöm riskerna för den registrerade och bedöm lämpliga tekniska och organisatoriska åtgärder
- Finns personuppgiftsbiträden?
- Genomför konsekvensbedömning
- Förhandssamråd med IMY
- Hur ska tester och uppföljning genomföras?





Medskick

- Förstå produkten
- Kartlägg användning
- Bedöm, utvärdera och hantera riskerna
- Följ upp, utvärdera och anpassa
- Våga använda ny teknik!

Frågor?



Lästips

- Transkribering inom socialtjänsten (Rapport från IMYs sandlåda)
- AI på IMY.se Artificiell intelligens (AI) | IMY
- Användning av AI i sjukvården | Medicinteknik | Läkemedelsverket
- Medical devices MDCG 2025-6

IMY. Integritetsskydds myndigheten

LÄKEMEDELSVERKET
SWEDISH MEDICAL PRODUCTS AGENCY

Tack för att du lyssnat! Svara gärna på vår utvärdering

