HELSE VEST IKT

Høringssvar til HITR 1252 *høringsutkast* 2023

Avsender: Helse Vest IKT

Vi takker for muligheten til å komme med innspill til høringsutkastet HITR 1252 «Bruk av direkte identifiserbare helseopplysninger til utvikling og testing av behandlingsrettede helseregistre».

I tabellen under er det noen spesifikke tilbakemeldinger på steder i teksten som vi mener det må gjøres noe med. Utgangspunktet er veldig bra, men det er noen saker som vi tenker kan gjøre dokumentet enda bedre og tydeligere:

- Begrepsavklaringer: Vi ser at det begrepsavklaringer i siste kapittel med fordel kan nevnes tidligere i innledningen f.eks. I tillegg at man legger inn en referanser til kapittelet der begrepene blir brukt.
- Dokumentet trengs å bli enda tydeligere i forhold til kravene, og flere plasser trengs det at ordet «bør» endres til skal eller må, se mer i tabellen under. Av erfaring ser vi at ordet «bør» så lett kan brukes som et argument for at man ikke trenger å forholde seg til det. Om man opplever å bruke ordet skal som belastende, må setningene eventuelt skrives om slik at det fremmer mer krav enn ønske.
- Generelt i dokumentet er det litt uklart om det er de samme reglene som gjelder for personopplysninger og direkte identifiserbare helseopplysninger, evt hvilke regler/retningslinjer som skal gjelde for hva.
- Gjelder disse retningslinjene på samme måte for automatiserte tester hvor det er en maskin og ikke en person som ser person/helseopplysninger?
- Vi synes og det er problematisk at prøvedrift blir definert under test begrepet, og mener at dette må tas ut av testbegrepet, og omtales i egne dokumenter som omhandler verifisering i produksjon. I arbeidet med *Overordnet ROS-vurdering av datakvalitet, test og opplæring i produksjon* i mars 2019 ble det forankret at aktiviteter som kan foregå i produksjon er verifisering ved prodsetting, mens test og kurs skal foregå i egnede miljøer.

I vedlagte PDF har vi markert teksten der vi mener det må endringer, justeringer eller slettinger til, i tillegg har vi i tabellen under lagt inn teksten som er markert gult i pdf'en, og lagt inn kommentarer der vi mener det må spesifiseres mer, eller forslag til endring i tekst.

Kapittel	Side nr. & paragraf	Tekst	Kommentar/endringer
1.1 Bakgrunn	s. 5, 2. paragraf, Siste setning	Det følger blant annet at begrepet «prøvedrift i denne sammenhengen vil være omfattet av begrepet "test".»	Det må spesifiseres nærmere hva som menes med "prøvedrift", er det pilot eller godkjenningsperiode. Drift gir inntrykk av at det gjelder prodmiljøet, der andre regler gjelder. Vi mener at dette ikke vil

			være omfattet av begrepet «test».
1.1 Bakgrunn	s 5, siste paragraf	Dersom en virksomhet velger å ikke følge anbefalingene i retningslinjen, bør dette være basert på en konkret og begrunnet vurdering. Begrunnelsen for å fravike retningslinjen bør dokumenteres.	**Endres** til «retningslinjen, skal dette være basert på en konkret og begrunnet vurdering» «retningslinjen skal dokumenteres»
1.2 Om retningslinjen	s 6, 1 paragraf	Retningslinjen beskriver videre hvilke sikkerhetstiltak som bør iverksettes i forbindelse med bruk av helseopplysninger til utviklings- og testformål. Dette omfatter:	**Endres** til «sikkerhetstiltak som må iverksettes»
2. Vilkår for å bruke --	s 7, punktliste	• Utviklingen og testingen må skje i et lukket testmiljø	- Her trengs det å definere tydeligere hva som menes med lukket testmiljø. Helt isolert? Ingen knytninger til andre fagsystem internt?, eller gjelder det koblinger til eksterne parter?
2. Vilkår for å bruke --	s 7, 3. paragraf	Virksomheten kan bare benytte helseopplysninger dersom det vil være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å benytte fiktive, anonymiserte eller pseudonyme helse- og personopplysninger.	Behov for definisjon av uforholdsmessig. Presisere at tid og kost ikke faller inn under uforholdsmessig.
2.1.2 Vilkår 2: Uforholdsmessig vanskelig - Oppfyllelse av pasientrettigheter	s. 9, 2 paragraf, siste del.	kan dette være et moment som tilsier at utviklings- eller testaktiviteten ikke ~~bør~~ gjennomføres med helse- og personopplysninger.	Enten ta bort, eller erstatt med kan – «testaktiviteten ikke (kan) gjennomføres med»
3.1 Utvikling, testing og prøvedrift	s. 10, siste paragraf første del	Med prøvedrift menes den innledende fasen etter at et utviklings-	**Prøvedrift** må som nevnt defineres mye tydeligere,

		eller testløp er ferdigstilt, og hvor systemet er i produksjon for å kontrollere at funksjonaliteten er tilfredsstillende.	og må følge gjeldende regler for Produksjon. Prøvedrift og verifisering er aktiviteter relatert til prodsetting, og vi mener at dette ikke bør være en del av dette dokumentet, men omtales spesifikt i et eget dokument.
3.1 Utvikling, testing og prøvedrift	s. 10, siste paragraf siste setning	«…. kunne komme til anvendelse, da det følger av forarbeidene at «prøvedrift i denne sammenhengen vil være omfattet av begrepet "test".»	**Endres** til "vil IKKE være omfattet av begrepet "test". Vi mener at prøvedrift ikke skal kobles sammen med test, da dette lett kan gi utilsiktede føringer for større muligheter til å teste i prodmiljøene.
3.2 Separate utviklings- og testmiljøer	s. 11, 1 paragraf	Testmiljøer bør også merkes tydelig, for å unngå at testsystemet blir benyttet ved pasientbehandling eller at det skjer testing i produksjonsmiljøet.	**Endres** til skal «Testmiljøer skal også merkes tydelig»
3.3 Kompetanse og taushetsplikt	s. 11 1. paragraf	Helsevirksomheten som er dataansvarlig for utviklingen eller testingen, bør utpeke en ressurs som har det operative ansvaret for ivaretakelse av informasjonssikkerhet og personvern under hele utviklings- og testfasen.	«for utviklingen eller testingen, skal utpeke en ressurs som har det operative ansvaret»
3.3 Kompetanse og taushetsplikt	s. 11 1. paragraf Siste setning	Personer som er involvert i databehandlingen må orienteres om taushetsplikten. Det kan for eksempel benyttes taushetserklæringer som signeres av den enkelte medarbeider.	Her bør man vel være litt mer tydelig på at det er viktig at taushetserklæringer må signeres. Er det tilstrekkelig at de bare informeres? I Helse Vest har vi som krav at leverandør må ha signert taushetserklæring for å få tilgang.
3.4 Dataflyt	s. 11, 1 paragraf	Det bør derfor utarbeides detaljerte	**Endres** til «Det må derfor utarbeides…..»

		oversikter over dataflyten i begge miljøene, for eksempel i et dataflytskjema	
3.4 Dataflyt	s. 12, 1 paragraf	Hvis en leverandør eller andre eksterne parter har tilgang til utviklings- og testmiljøet, bør dette inngå i dataflytskjemaet.	**Endres** til «…tilgang til utviklings- og testmiljøet, er det viktig at dette inngår i dataflytskjemaet
3.4 Dataflyt	s. 12, siste paragraf	Det kan også være behov for å benytte perifert utstyr i forbindelse med utvikling eller testing (BYOD, medisinsk utstyr, mobiltelefoner mv.).	**VIKTIG:** Da det er behov for å ha oversikt over hvem og hvilke tilganger som er gitt til identifiserbare helseopplysninger så skal ikke BYOD være et alternativ. Bruk av BYOD vil gi en økt risiko for misbruk av data!
3.5 Testplan	s. 12, 1. paragraf	Virksomheten bør etablere en utviklings- og testplan, som kan inneholde en beskrivelse av aktivitetenes formål, omfang, fremgangsmåte, ressurser og fremdriftsplan.	**Endres** til «Virksomheten bør etablere en utviklings- og testplan, som inneholder en beskrivelse av aktivitetenes formål, omfang, fremgangsmåte, ressurser og fremdriftsplan.
3.5 Testplan	s. 12, 1. paragraf	I planen bør utviklings- og testobjektene defineres, og man bør beskrive hvilke egenskaper som skal testes, hvilke oppgaver….	**Endres** til «I planen skal utviklings- og testobjektene defineres, og man beskriver hvilke egenskaper som skal testes, hvilke oppgaver….»
3.6 Vurdere datagrunnlaget	s. 12, 2. paragraf	Dersom uttrekket kan omfatte opplysninger der det er vurdert til at pasienten selv ikke har rett til innsyn, bør det vurderes om bruk av dataene til utvikling eller testing vil kunne gi risiko for innsyn via innsyn i testdataene, se kapittel 3.9.	**Endres** til «… selv ikke har rett til innsyn, skal det vurderes om bruk av dataene til utvikling eller testing vil….»

3.7 Risikovurdering og personvernkonsekvens vurdering	s. 13 1. paragraf	Slike vurderinger kan virksomheten utføre i en risiko- og sårbarhetsanalyse og i en personvernkonsekvensvurdering (DPIA).	**Endres** til «Slike vurderinger utfører virksomheten i en risiko- og sårbarhetsanalyse og i en personvernkonsekvensvurdering (DPIA).»
3.8 Tilgangsstyring og kontroll	s. 13 siste paragraf	For å sikre at det skilles mellom tilganger til testmiljøer og vanlige brukertilganger, er det viktig at det opprettes egne brukerkontoer for testing (testkontoer). Dette er også viktig for å ivareta krav til logging, se kapittel 3.9 nedenfor.	**Endres** til «For å sikre at det skilles mellom tilganger til testmiljøer og vanlige brukertilganger, skal det opprettes egne brukerkontoer for testing (testkontoer). Dette er også viktig for å ivareta krav til logging, se kapittel 3.9 nedenfor.» - Det er og viktig å tydeliggjøre om dette også gjelder testmiljø som inneholder pseudonymiserte/anonymiserte testdata