1. Hensikt/omfang

Test av IT-løsninger er en sentral del av arbeidet ved utvikling av nye IT systemer og integrasjoner, ved oppgraderinger og ved feilsøking. Hensikten med denne prosedyren er å sikre testing utføres med minimal inngripen i personvern og med god informasjonssikkerhet.

2. Ansvar/målgruppe

Utforming/vedlikehold av rutinen: Utvalg for regional IKT-sikkerhet

Utførelse: Prosjekt/testleder har ansvar for etterlevelse av tiltak i denne rutinen, og besørge at disse er kjent for de som deltar i testen

3. Gjennomføring

Gjennomføringen henspeiler på bruk av testdata som ved behov nødvendiggjør bruk av reelle personopplysinger i systemet.

Retningslinjer for bruk av testdata

Ved bruk av personopplysninger ved test skal det alltid tas utgangspunkt i bl.a. det grunnleggende personvernprinsippet i personvernforordningen art 5 b) «dataminimering». Det skal kun brukes adekvate og relevante personopplysninger og det skal begrenset til det som er nødvendig for formålet for behandlingen/testen.

Følgende retningslinjer gjelder for *alle* som gis tilgang til testmiljø som inneholder direkte og indirekte identifiserbare personopplysninger:

- Bruk ikke mer reelle data enn det er behov for (konkretisering: dersom reelle data må brukes skal det vurderers å bruke en mindre gruppe/et mindre datasett, ikke hele databasen i testsettet)
- Bruk fiktive testdata der det er mulig
- Verken personopplysninger eller pasientopplysninger skal diskuteres med andre

- Følgende data skal *ikke brukes* til test:

- sperrede pasientjournaler eller sperrede personopplysninger
- data fra pasienter eller registrerte man kjenner
- data fra offentlig kjente personer

Bakgrunn

Det er viktig at testaktivitetene gjenskaper virkeligheten så godt som mulig, slik at feil og mangler i løsningen kan finnes i forkant av produksjonssetting. Dette gjør det nødvendig å benytte relevante testdata (i noen tilfeller også personidentifiserbare personopplysninger) for å sikre kvalitet på testaktivitetene.

Det presiseres at personopplysninger som ikke er anonymisert, og som brukes i testformål, skal behandles som personopplysninger (eventuelt også som helseopplysninger). Dette medfører krav om at systemer som inneholder denne informasjonen må bli behandlet etter krav stilt i gjeldende lovgivning (personvernforordningen, pasientjournalloven, helseregisterloven med flere). Det vises spesielt til krav om tilgangsstyring, logging av oppslag m.m. I praksis vil dette kunne ivaretas ved at man setter samme sikkerhetskrav til testmiljøer som til produksjonsmiljøer.

I testmiljøets levetid skal direkte og indirekte identifiserbare testdata sikres i henhold til avtalte rutiner mht. konfidensialitet, integritet og tilgjengelighet.

Aktiviteter

Aktivitet	Oppgave
Testforberedelser	**Prosjekt/testleder** • Beskrive formålet med og varigheten av testen • Skal opprette og vedlikeholde en oversikt over hvem som deltar i testen, hvilke rettigheter de har, at taushetsplikten er ivaretatt og at eLæringsmodul Informasjonssikkerheter bestått. • Autorisasjonene som gis skal være tidsbegrenset, og rettighetene i forhold til den enkelte testers behov / rolle. • Prosjekt-/testleder må innhente tidsbegrenset tillatelse fra involvert(e) foretak (databehandlingsansvarlige) i forkant av gjennomføring av tester. IKT-Sikkerhetsleder i hvert foretak er kontaktperson for disse henvendelsene. Prosjekt-/testleder kan først undersøke om gjeldende databehandleravtale gir tillatelse til gjennomføring av testen. • Den enkelte testbruker skal tildeles en egen personlig testrolle med brukernavn og passord og ikke benytte sin ordinære autorisasjon. • Virksomheten som eier dataene skal til enhver tid ha oversikt over hvem som har tilgang til testområdet og hvilke rettigheter de har • Det skal gjennomføres en risikovurdering før bruk av testdata • Påse at fysisk og logisk sikring er ivaretatt **Deltager i test** • Skal på eget initiativ påse at taushetsplikten er formalisert ved at Taushetserklæringsskjema er undertegnet og eLæringsmodul for Informasjonssikkerhet er bestått. • Avbryte test dersom man kommer i kontakt med data fra pasienter eller personer man kjenner **Øvrige oppgaver**

	• Dersom eksterne parter (databehandler, leverandør, virksomhet) gis tilgang til et testmiljø med personidentifiserbare personopplysninger skal det være opprettet en skriftlig avtale om bruk av testdata, ref. punktet over om å innhente tillatelse fra virksomheten **Systemsikkerhet** • Tilse at alle relevante deltakere med behov for ekstern tilgang til testdata benytter gjeldende løsning for fjernaksess i Helse Vest. Videre har man samme krav til autentisering for slik tilgang som for tilgang til tilsvarende produksjonsdata. • Bærbart utstyr skal være sikret i tråd med krav i styringssystemet • Dersom personopplysninger må tas eller kopieres ut av testsystemene for konvertering, bearbeiding eller analyse osv skal det opprettes et eget tilgangsstyrt område for evt. midlertidig lagring av disse personopplysningene. IKT-sikkerhetsleder i virksomheten kan kontaktes for å beslutte rett sikkerhetsnivå. • Det bør etableres enten et fysisk eller logisk (logiske adskilt database) skille mellom produksjonsmiljø og testmiljø om testen ikke skal foregå i produksjonsmiljøet **Prosedyrer** • Ved etablering av testdata skal det utarbeides prosedyre for: • Uttrekk av testdata fra eksisterende registre (for eksempel EPJ-system) • Anonymisering av testdata • Pseudonymisering / etablering av indirekte identifiserbare testdata • Bruk av testdata • Tilgangsstyring til testdata og logging av tilgang • Overføring av testdata til andre (databehandler, leverandør, virksomhet) • Forankre bruk av identifiserende eller indirekte identifiserbare testdata hos personvernombud, herunder gjennomføring av personvernkonsekvensvurdering • Sletting av testdata etter at test er gjennomført
Testgjennomføring	• Prosessen med utplukk av testdata skal sikres etter krav i styringssystemet • Ved bruk av testdata skal vi i størst mulig grad ivareta at den minst personverninngripende løsningen som kan ivareta det angitte formålet med databehandlingen velges • Utplukksregler skal beskrives iht det fastsatte formålet

	• Test på reelle data:
	  • Før testen skal det verifiseres at det er tatt sikkerhetskopier og at det fins prosedyrer for tilbakekopiering om testen korrumperer data
	  • Det skal føres logg over oppslag.
	
	• Det anbefales å føres manuelle logg over endringer for å kunne spore uønskede hendelser til konkrete operasjoner og tidspunkter
	• Alle oppslag i pasientjournaler blir logget i tråd med gjeldende praksis i fagsystemet som det skal testes på
	• I logg skal testbrukeren registreres med egen rolle for testing slik at det ved analyse av loggen ikke fremstår som om testbrukeren har utført ulovlige handlinger
	• Databehandlingsansvarlig har innsynsrett i loggene
	• Utskrifter som inneholder personopplysninger skal sikres ved innlåsing, enten i skuffer, skap eller ved låsing av kontor. Utskrifter skal etter bruk makuleres/avhendes på forsvarlig måte etter at formålet med utskriften er oppnådd.
	• Unngå bruk av flyttbare lagringsmedia. Disse skal i tilfelle sikres etter krav i styringssystemet
	• Vedlegg med personopplysninger skal ikke sendes per usikret epost, man kan sende en peker/referanse til saksnummer i HP ALM.

Prosedyre for tilganger	• Tilgangsbehandling i Helse Vest IKT administrerer brukerkontoer i Helse Vest, og blir dermed også de som oppretter og fjerner tilganger for midlertidige testbrukere.
	
	  • *Styring av brukertilganger*
	  ◦ Oversikter over hvem som har tilgang ligger i AD
	  ◦ Ansvarlig for oppdatering gjøres av Tilgangsbehandling, på basis av bestillinger i Kundeweb/Assyst fra prosjekt/testleder
	  • *Melde nye brukere*
	  ◦ Bestilling av nye brukere meldes i Kundeweb/Assyst av prosjekt/testleder ved oppstart av test.
	  • *Melde om fjerning av tilgang*
	  ◦ Når testperioden er ute, eller når formålet med testen er oppnådd gir prosjekt/testleder beskjed til Tilgangsbehandling om at testbrukerene kan deaktiveres.
	  • *Kontrollrutiner på at deaktivering av testbrukere er utført*
	  ◦ Deaktivering dokumenteres ved at

	Tilgangsbehandling dokumenterer aktiviteten i aktuell(e)Assyst-sak(er), samt at melding sendes til relevant personell hos involverte helseforetak via Kundeweb. «Dette vil da være tilgjengelig i Kundeweb og Assyst, og dokumentasjonen på at jobben er gjort vil være tilgjengelig både for personell i HVIKT og hos Databehandlingsansvarlig/foretakene.» • *Dokumentasjon* ◦ Oversikt over hvem som har tilgang til testdataene i det enkelte system i testmiljøet oppbevares av Databehandler ved prosjekt/testleder. Opplysningene skal alltid være tilgjengelig for Databehandlingsansvarlig for tilsvarende produksjonsdata på forespørsel.
Avviksrapportering	• Mistenkelige hendelser og observerte brudd på personopplysningssikkerheten skal rapporteres til nærmeste leder og/eller IKT-sikkerhetsleder. Gjeldende avviksrutiner skal følges. • Hendelser knyttet til at virksomhetens sikkerhetsinstruks ikke følges, vurderes også som sikkerhetsbrudd. Brudd på sikkerhetsinstruks ses på som mislighold av arbeidsavtalen og virksomhetens styringssystem for IKT-sikkerhet, og vil kunne bli behandlet som en personalsak. Alvorlige brudd på reglene i sikkerhetsinstruksen vil få konsekvenser for ansattes arbeidsforhold samt eventuelt resultere i strafferettslige reaksjoner.
Avslutning/opp-rydding etter test	• Testdata slettes når avtalt sluttidspunkt for bruk er nådd eller når testen er gjennomført • Logger fra test arkiveres • Utskrifter skal makuleres • Ansvarlig for bruk av testdata skal sende bekreftelse til databehandlingsansvarlig at alle testdata er slettet i henhold til formål og avtale • Testmiljøet fjernes, dersom dette er hensiktsmessig • Tilgangsbehandling får beskjed om at testbrukere skal deaktiveres

-

4. Referanser

Nr	Kilde	Merknad

1.	Personverforordningen	• Art 32 Sikkerhet ved behandlingen
2.	Pasientjournalloven	• § 22. *Sikring av konfidensialitet, integritet og tilgjengelighet*
3.	Helseregisterloven	• § 21. *Sikring av konfidensialitet, integritet og tilgjengelighet*