NORMEN

Testing og testdata (faktaark 43)

Versjon 3.0

29.mars 2022

Utarbeidet med støtte fra direktoratet for e-helse

Vedtatt av styringsgruppen for Normen

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler testing og testdata. Formålet med faktaarket er å sikre at informasjonssikkerhet og personvern blir ivaretatt ved testing i forbindelse med utvikling og endring av systemer som behandler helse- og personopplysninger. Faktaarket er avgrenset til testing i forbindelse med utvikling av nye systemer og endring av eksisterende systemer. Faktaarket omhandler ikke sikkerhetstesting i produksjonsmiljøet.[1]
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er er virksomheter som behandler helse- og personopplysninger. Faktaarket vil særlig være relevant for personell som har fått delegert det daglige ansvaret for at informasjonssikkerhet og personvern ivaretas ved utførelser av tester. Dette kan for eksempel være en IKT-ansvarlig og avdelingsleder hvor testingen gjennomføres.
Krav i Normen 6.0	Faktaarket gjelder for følgende kapitler i Normen 6.0 • Norm for informasjonssikkerhet kap. 5.4.1 Konfigurasjonskontroll
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: • Personvernforordningen artikkel 5 Prinsipper for behandling av personopplysninger • Personvernforordningen artikkel 6 Behandlingens lovlighet • Personvernforordningen artikkel 9 Behandling av særlige kategorier av personopplysninger • Personvernforordningen artikkel 28 Databehandler • Personvernforordningen artikkel 35 Vurdering av personvernkonsekvenser • Personvernforordningen artikkel 32 Sikkerhet ved behandlingen • Pasientjournalloven § 22 Informasjonssikkerhet • Helseregisterloven § 21 Informasjonssikkerhet • Personvernforordningen kapittel III Den registrertes rettigheter (artikkel 12-22) • Håndbok i beskyttelse av skjermingsverdig ugradert informasjonssystem - 5.3.5 testing, Nasjonal sikkerhetsmyndighet (NSM) • NSMs grunnprinsipper for IKT-sikkerhet 2.0, prinsipp 2.1.6 og 2.1.7

[1] NSMs grunnprinsipper for IKT-sikkerhet grunnprinsipp 3.4

	• Sikring av bærbart utstyr (faktaark 18) • Hjemmekontor og annet fjernarbeid (faktaark 29) • Håndtering av lagringsmedia (faktaark 34) • Personvernprinsipper (faktaark 57) • Veileder for fjernaksess mellom virksomhet og leverandør • Veileder i bruk av skytjenester til behandling av helse og personopplysninger • Veileder for rettigheter ved behandling av helse og personopplysninger. •

Testing og testdata

Testing er en sentral del av utviklingsarbeidet med nye systemer eller endringer på eksisterende systemer. For å oppnå mest mulig effektiv testing er det nødvendig å benytte relevante testdata slik at testene blir så nær opp til virkeligheten som mulig. Bruk av helse- og personopplysninger til testing vil imidlertid utgjøre et inngrep i den enkeltes personvern. Hovedregelen er derfor at testing skal gjennomføres med syntetiske data, det vil si fiktive data som er laget for testformål.

Helse- og personopplysninger kan benyttes til testing unntaksvis dersom det er nødvendig. I slike tilfeller må virksomheten etterleve en rekke krav til informasjonssikkerhet og personvern. Dette faktaarket gir en beskrivelse av ulike typer testdata og hvordan virksomheten bør gå frem for å ivareta krav til informasjonssikkerhet og personvern ved bruk av helse- og personopplysninger som testdata. Formålet med faktaarket er å sikre at informasjonssikkerhet og personvern blir ivaretatt ved utvikling og testing av IT-systemer.

Rammer og metodikk for testing i helse- og omsorgssektoren varierer ut ifra virksomhetenes størrelse og kompleksitet. Rådene i dette faktaarket er ment å gjelde for både små og store virksomheter. Virksomheter som har ressurser til det anbefales å benytte et eget rammeverk for testmetodikk.

Faktaarket inkluderer og erstatter det som tidligere var faktaark 48 - Informasjonssikkerhet ved utførelse av testing.

Innhold

1. Hovedregel om separat testmiljø

I Normen er det fastsatt krav om at det skal benyttes separate miljøer for utvikling, test og produksjon slik at helse- og personopplysninger som benyttes ved ytelse av helsehjelp ikke blir påvirket ved feil i utvikling og test.[2]

Eksempler på scenarioer som kan inntreffe dersom det ikke benyttes separate[3] miljøer ved testing kan være:

- Utvikler av et journalsystem får tilgang til pasientopplysninger som vedkommende ikke skulle hatt tilgang til (konfidensialitet).
- En pasientjournal inneholder feil data som følge av at testdata er benyttet i produksjon (integritet & pasientsikkerhet).
- Ufullstendig testing fører til at helse- og personopplysninger blir utilgjengelige (tilgjengelighet).

Et testmiljø etableres som en permanent løsning eller ha en tidsavgrenset varighet.

Testmiljøet skal sikres avhengig av hva slags type data som benyttes ved testing.[4] Dersom virksomheten for eksempel benytter helse- og personopplysninger fra produksjonsmiljøet til testformål, stilles det samme krav til sikring av testmiljøet som til produksjonsmiljøet.[5][6]

Testing i produksjonsmiljøet skal ikke forekomme, annet enn hvis det er strengt nødvendig, som følgende eksempler.

- dersom det er nødvendig for kvalitetssikring av helse- og personopplysningenes integritet ved systemendringer[7]
- ved bytte av system eller leverandør som medfører konvertering av helse- og personopplysninger, hvor hovedregelen er at både konvertering og test av resultatet må foretas på reelle data for å kunne teste en fullstendig konvertering[8]
- ved test av nye og eksisterende integrasjoner mot andre produksjonssystemer hvor det ikke finnes testmiljøer og er nødvendig med tilnærmet fullstendige og reelle data, for å kunne få til en realistisk kommunikasjonstest med eksterne parter
- etter konfigurasjonsendringer eller oppdateringer på eksisterende applikasjoner som behandler helse- og personopplysninger i eksisterende produksjonssystemer, hvor det ikke finnes et separat testmiljø.

Det er viktig å være oppmerksom på at situasjonene som er beskrevet ovenfor er å regne som unntak og skal ikke innarbeides som fast praksis. Dersom noen av situasjonene er aktuelle skal virksomheten planlegge for dette ved å gjennomføre risikovurderinger og

[2] Normen 6.0 kap. 5.4.1
[3] Dvs at man systemteknisk skiller produksjonsmiljø, utviklingsmiljø og testmiljø fra hverandre.
[4] NSMs grunnprinsipper for IKT-sikkerhet tiltak 2.1.6 i kombinasjon med tiltak 2.2.3.
[5] Se for eksempel krav til sikkerhet, tilgangstyring og logging i personvernforordningen artikkel 32, pasientjournalloven § 22 og helseregisterloven § 21
[6] Se også ROS analyse - Vurdering av datakvalitet test og opplæring i produksjon fra mars 2019.
[7] Prosess og rutiner bør legge prinsipper om endringsstyring i NSMs grunnprinsipper for IKT-sikkerhet tiltak 2.10 til grunn.
[8] NSMs grunnprinsipper for IKT-sikkerhet tiltak 2.1.10 j)

implementere tiltak for å håndtere, eksempelvis gjennom definerte tekniske og organisatoriske tiltak og rutiner.[9]

2. Ulike datagrunnlag ved testing

Virksomheten kan benytte ulike typer data ved testing; helse- og personopplysninger fra produksjonsmiljøet, syntetiske data, anonymiserte data eller pseudonymiserte data. Utgangspunktet ved testing er at det skal brukes syntetiske data. Test i produksjon skal begrenses til ren verifisering uten modifisering på reelle data.

2.1 Syntetiske data

Syntetiske data er fiktive opplysninger som er laget for testformål. Syntetiske data kan ikke identifisere fysiske personer og anses derfor ikke som personopplysninger. Behandling av syntetiske data er ikke underlagt kravene til behandling av helse- og personopplysninger i personvernforordningen og særlovgivningen for helse- og omsorgssektoren. Bruk av syntetiske data medfører heller ingen risiko for den enkeltes personvern. Som hovedregel gjennomføres testing med syntetiske data.[10]

For å sikre god nok testing av systemene og at alle scenarioer blir testet, er det viktig å sørge for at de syntetiske dataene gjenspeiler virkeligheten og at det er variasjon i dem. Dersom testdataene ikke er gode nok, kan testingen av systemene bli mangelfull. Dette kan igjen gå utover pasientsikkerheten når helse- og personopplysninger skal behandles i systemene.

2.2 Anonymiserte data

Med anonymiserte data menes helse- og personopplysninger der navn, fødselsnummer og andre personentydige kjennetegn har blitt fjernet, slik at opplysningene ikke lenger kan identifisere fysiske personer.[11] Dette betyr at betyr at alle muligheter for re-identifisering av dataene er fjernet. Når data er anonymisert anses ikke lenger opplysningene å være personopplysninger. Behandling av anonymiserte data må derfor ikke følge kravene til behandling av helse- og personopplysninger i personvernforordningen og særlovgivningen for helse- og omsorgssektoren.

Anonymisering kan være en metode for å redusere risikoene knyttet til behandling av helse- og personopplysninger. Det er imidlertid viktig å være oppmerksom på at prosessen med anonymisering i seg selv er en behandling av personopplysninger som forutsetter at kravene til behandling av helse- og personopplysninger er oppfylt.[12] Anonymisering kan også være vanskelig å gjennomføre i praksis. I de fleste tilfeller er det derfor mer effektivt å produsere syntetiske testdata enn å anonymisere helse- og personopplysninger for bruk i test.

2.3 Pseudonymiserte data

Med pseudonymiserte data menes helse- og personopplysninger hvor identifiserende opplysninger er erstattet slik at de ikke kan identfisere en fysisk person uten bruk av

[9] NSMs grunnprinsipper for IKT-sikkerhet tiltak 1.1.4 sammen med 4.1.1 og 4.1.2
[10] Datatilsynet veileder for programvareutvikling med innebygd personvern punkt 7
[11] Personvernforordningen fortalepunkt 26
[12] Dataansvarlig må blant annet vurdere om behandlingen er forenlig med de opprinnelige formålene eller om det finnes et annet behandlingsgrunnlag for anonymiseringen.

tilleggsopplysninger.[13] Ettersom pseudonymiserte opplysninger kan identifisere fysiske personer dersom opplysningene sammenstilles, anses pseudonymiserte data som personopplysninger. Behandling av pseudonymiserte opplysninger må derfor følge krav til behandling av helse- og personopplysninger i personvernforordningen og særlovgivningen for helse- og omsorgssektoren. Pseudonymiserte data er det mest vanlige resultatet for testdata som anonymiseres, da de fleste leverandører ikke har anonymiseringsrutiner som gjør en fullverdig anonymisering.

For mer informasjon om pseudonymisering henvises til The European Union Agency for Network and Information (ENISA) sin publikasjon om temaet.[14]

2.4 Helse- og personopplysninger i testmiljø med kopi av reelle data fra produksjon

Helse- og personopplysninger fra produksjonsmiljøet er opplysninger som kan identifisere fysiske personer. Behandling av slike data må derfor følge krav til behandling av helse- og personopplysninger i personvernforordningen og særlovgivningen for helse- og omsorgssektoren.

Bruk av helse- og personopplysninger til testformål medfører en risiko knyttet til informasjonssikkerhet og personvern. Slik bruk kan blant annet medføre at personell som driver med systemutvikling og systemvedlikehold får tilgang til helse- og personopplysninger som de i utgangspunktet ikke skal ha tilgang til, for eksempel at en utvikler av et journalsystem får tilgang til pasientopplysinger. Videre er test- og utviklingsmiljøer ofte ikke like godt sikret som produksjonsmiljøer, derfor må testmiljøer med reelle data sikres på samme måte som produksjon med tilsyn til tilgangskontroll, logging og overvåking. Det må sikres at pasienten kan få innsyn i loggene i henhold til gjeldende lovverk. Reelle helse- og personopplysninger benyttes kun unntaksvis og ved godkjente scenario til testformål.

3. Bruk av reelle helse- og personopplysninger som testdata

3.1 Krav til nødvendighet

Helse- og personopplysninger kan bare brukes for testformål dersom det er nødvendig.[15] Før virksomheten kan bruke helse- og personopplysninger til testing må det derfor vurderes om det er mulig å oppnå formålene med testingen ved bruk av syntetiske data, eventuelt anonymiserte eller pseudonymiserte opplysninger. Å gjøre slike vurderinger kan være krevende. Det er derfor viktig å involvere personell med relevant kompetanse og om nødvendig søke ekstern bistand, for å avklare hvordan pasientsikkerhet og personvern kan ivaretas. Dersom virksomheten har et personvernombud, kan dette involveres ved vurderingene. Vurderingene skal dokumenteres for etterkontroll.

[13] Personvernforordningen artikkel 4 nr. 5
[14] https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices
[15] Personvernforordningen 5 nr. 1 bokstav c

I tillegg til å vurdere nødvendigheten knyttet til bruk av helse- og personopplysninger til testing, må virksomheten også sørge for å oppfylle andre krav i personvernforordningen. Virksomheten må blant annet

- sikre at det finnes et rettslig grunnlag for å benytte helse- og personopplysningene til testing[16]
- sikre at personvernprinsippene etterleves[17]
- gjennomføre risikovurderinger[18] og personvernkonsekvensvurderinger[19]
- etablere sikkerhetstiltak for å beskytte opplysningene mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade[20]
- sikre at de registrerte får den informasjonen de har rett på om behandlingen[21]
- sørge for å ivareta de registrertes rettigheter, herunder retten til innsyn, retting og sletting[22]
- føre protokoll over behandlingen[23]
- sikre at eventuelle databehandlere som kan få tilgang til opplysningene oppfyller kravene i personvernforordningen og i Normen[24]
- sikre at det foreligger en skriftlig databehandleravtale med eventuelle databehandlere som gjennomfører testing[25]

3.2 Rutiner for bruk av helse- og personopplysninger som testdata

Nr.	Handling
1	**Forberedelser** a) Vurder om det er nødvendig å gjennomføre testen med helse- og personopplysninger for å oppnå formålet. Vurderingen skal dokumenteres.[26] b) Vurder hvilket rettslig grunnlag som ligger til grunn for behandlingen. Vurderingen skal dokumenteres.[27]

[16] Personvernforordningen artikkel 6 og 9. Se Formål og behandlingsgrunnlag (faktaark 56).
[17] Personvernforordningen artikkel 5. Se Personvernprinsippene (faktaark 57)
[18] Personvernforrodningen artikkel 32
[19] Personvernforordningen artikkel 35
[20] Personvernforordningen artikkel 32
[21] Personvernforordningen artikkel 12-14. Se veileder for rettigheter ved behandling av helse- og personopplysninger.
[22] Personvernforordningen artikkel 15-22. Se veileder for rettigheter ved behandling av helse- og personopplysninger.
[23] Personvernforordningen artikkel 30
[24] Personvernforordningen artikkel 28
[25] Personvernforordningen artikkel 28
[26] Personvernforordningen artikkel 5 nr. 1 bokstav c, jf. artikkel 24
[27] Personvernforordningen artikkel 6 og 9, jf. artikkel 24

Nr.	Handling

	c) Avklar ansvar og arbeidsoppgaver til ulike roller internt i virksomheten og hos eventuell ekstern part.
	d) Dersom testen skal gjennomføres av en ekstern part, skal det inngås en skriftlig databehandleravtale med denne.[28] I tillegg til å oppfylle kravene i personvernforordningen artikkel 28, er det viktig at databehandleravtalen beskriver:
	- testens varighet
	- databehandlers forpliktelse til å følge krav i Normen
	- hvem som er ansvarlig for hva under gjennomføring av testen (f.eks. prosjektleders rolle)
	- beskrivelse av om separat testmiljø benyttes eller om det skal utføres test på data i produksjonsmiljø
	- hvem som skal ha tilgang til testdataene og rutiner for tilgangsstyring
	- at de som gjennomfører testen skal være underlagt taushetsplikt
	- at det skal gjennomføres risikovurderinger knyttet til bruk av helse- og personopplysninger i testen
	- tiltak for fysisk og logisk sikring
	- at opplysningene skal slettes når testen er avsluttet og at databehandler skal bekrefte sletting
	- hvilke særskilte rutiner som gjelder
	e) Gjennomfør risikovurderinger og personvernkonsekvensvurderinger, og etabler egnede sikkerhetstiltak.[29] Virksomheten skal blant annet hensynta:
	- antall registrerte og omfanget av helse- og personopplysninger i testdataene
	- antall ansatte som skal ha tilgang til testdata
	- testens varighet
	- de registrertes mulighet til å utøve sine rettigheter
	- testmiljøet
	  ○ fysisk og logisk skille mellom testdata og helse- og personopplysninger
	  ○ fysisk og logisk driftsmiljø
	- tilgangsstyring, logging og oppfølging av tilgangsstyringen
	f) Utarbeid rutiner for:
	- utplukk av testdata fra eksisterende registre (for eksempel EPJ-system)
	- tilgangsstyring til testdata og logging av tilgang
	- bruk av testdata

[28] Personvernforordningen arikkel 28
[29] Personvernforordiningen artikkel 32 og 35

Nr.	Handling
	- overføring av testdata til andre (databehandler, leverandør, annen helse- eller omsorgsvirksomhet).[30] - sletting av testdata etter at test er gjennomført g) Etabler teknisk løsning for behandling av testdata. - Det skal som hovedregel etableres et eget testmiljø som er separert fra utvikling og produksjon.[31] Unntak fra dette må risikovurderes og håndteres basert på fastsatt akseptabelt risikonivå. - Testmiljøet skal sikres på tilsvarende måte som produksjonsmiljøet.[32] - Ved overføring av testdata til testmiljøer utenfor den dataansvarliges eget nettverk skal det etableres tekniske tiltak, slik at all kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll krypteres. Kryptering og dekryptering mellom kommunikasjonspunkter i infrastrukturen skal gjøres i godkjent utstyr som virksomheten har kontroll med. Kontrollen kan ivaretas gjennom avtale. - For testing av nasjonale løsninger vises det til Norsk Helsenett og nasjonal test- og godkjenningsordning.[33]
2	**Gjennomføring** a) Identifiser tilgjengelig datagrunnlag - Syntetiske og fullverdige anonymiserte data kan fritt brukes til testformål - Pseudonymiserte data underlegges samme krav til sikkerhet og logging som reelle data - Reelle data (kopi fra produksjon) underlegges samme krav til sikkerhet og logging som i produksjon, og skal kun benyttes der det er strengt nødvendig. Behov for bruk av reelle data skal vurderes av sikkerhetsansvarlig og personvernombud i det enkelte tilfelle og nødvendigheten skal dokumenteres. b) Plukk ut testdata til det konkrete formålet basert på datagrunnlaget iht. til fastsatt rutine. - Utplukksregler skal beskrives iht det fastsatte formålet - Datafelter og datamengde velges utfra reelt behov (dataminimering) - Det benyttes syntetiske, anonymiserte eller pseudonymiserte testdata dersom det er mulig - Testdataene skal sikres iht kravene i personvernforordningen og Normen c) Ved test i produksjonsmiljøet begrenses testingen til verfisering (f.eks ved prodsetting), og uten modfisering av data.Følgende tiltak må iverksettes:

[30] For overføring til virksomheter i utlandet, se http://www.datatilsynet.no/Sektor/Overfoering/
[31] Normen 6.0 kapittel 5.4.1
[32] NSMs grunnprinsipper for IKT-sikkerhet tiltak 2.1.6 om at testmiljøer hvor det behandles sensitive prosuksjonsdata skal sikres og krav til sikkerhet i personvernforordningen artikkel 32, pasientjournalloven § 22 og helseregisterloven § 21.
[33] https://www.nhn.no/samhandlingsplattform/andre-tjenester/meldingsvalidator-test-og-godkjenning

Nr.	Handling
	- Før testen gjennomføres skal det verifiseres at det er tatt sikkerhetskopier og at det finnes rutiner for tilbakekopiering dersom testen korrumperer data - Det skal føres logger og det anbefales å føre manuelle logger for å kunne spore uønskede hendelser til konkrete operasjoner og tidspunkter d) Sørg for tilgangsstyring og taushetsplikt. - Virksomheten skal føre oversikt over hvem som har tilgang til testområdet (testbrukere) og hvilke rettigheter de har - Virksomheten skal sørge for at testbrukere er underlagt taushetsplikt gjennom ansettelsesavtale eller ved særskilt skjema som signeres før oppstart av testen - Alle testbrukere skal tildeles en egen personlig testkonto - Alle testbrukere skal registreres med egen konto og rolle i logger slik at det ved analyse av logger ikke fremstår som om testbrukeren har utført ulovlige handlinger e) Andre tiltak virksomheten må påse at ivaretas for å sikre informasjonssikkerhet er: - At e-post ikke benyttes til å sende helse- og personopplysninger - At bærbart utstyr som benyttes til test av systemer med helse- og personopplysninger er sikret iht. Normens krav[34] - At testing utenfor egen arbeidsplass følger Normens krav for hjemmekontor og fjernaksess[35] - At trådløse nettverk er sikret[36] - At papirutskrifter, minnepinner og andre lagringsmedier som inneholder helse- og personopplysninger merkes, oppbevares og sendes iht. Normens krav[37] - At bruk av eventuelle skybaserte løsninger følger akutelle krav i Normen[38] - At feil og mangler som hovedregel ikke beskrives med identifiserbare helse- og personopplysninger. Beskrives feil og mangler med identifiserbare helse- og personopplysninger, skal datafiler og utskrifter sikres på samme måte som andre helse- og personopplysninger iht. krav i personvernforordningen og Normen - At alle avvik fra etablerte rutiner rapporteres som avvik iht. rutine for avviksbehandling f) Tester av sikkerhet og sikkerhetsfunksjoner før driftsetting:

[34] Sikring av bærbart (faktaark 18) hvor to av hovedtemaene er kryptering av lagringsmedia og sikkerhetsnivå 4 ved tilgang til helse- og personopplysninger
[35] Hjemmekontor og annet fjernarbeid (faktaark 29) og Veileder for fjernaksess mellom virksomhet og leverandør
[36] NSMs grunnprinsipper for IKT-sikkerhet 2.4
[37] Håndtering av lagringsmedia (faktaark 34)
[38] Se veileder i bruk av skytjenester til behandling av helse- og personopplysninger, som beskriver de spesielle risiko- og trusselområdene for bruk av skybaserte løsninger. Her finnes både konkrete innspill til databehandleravtale og sikkerhetstiltak ved bruk av skytjenester.

Nr.	Handling
	- Vurdere gjennomføring av tester av sikkerhet, som del av utvikling og test, før programvare settes i drift i virksomhetens produksjonsmiljø. Dersom produkter fra anerkjente produsenter[39] benyttes er behovet for sikkerhetstest mindre. Det er imidlertid spesielt viktig å teste egenutviklet programvare eller programvare som utvikles av en innleid leverandør. - Ved sikkerhetstester bør tester gjennomføres iht. NSMs grunnprinsipper for IKT-sikkerhet tiltak 2.1.7 *Gjennomfør tilstrekkelig testing gjennom hele utviklingsprosessen* og grunnprinsipp 3.4 *Gjennomfør inntregningstester* - Tester iht. grunnprinsipp 3.4 bør også gjennomføres periodisk i produksjonssystemer, men omtales ikke i dette faktaarket.
3	**Dokumentering og avslutning av test** a) Tester og verifikasjoner skal dokumenteres[40] som ledd i virksomhetens endringsstyring[41]. b) I testmiljøer med tidsavgrenset varighet skal testdataene slettes når formålet er oppnådd og eventuelle utskriftene skal makuleres etter bruk. c) I permanente testmiljøer skal testdata som ikke lenger har et formål slettes. Eventuelle utskrifter makuleres. d) Ved bruk av databehandler for å gjennomføre testen, skal databehandler sende bekreftelse til dataansvarlig om at alle testdata er slettet iht. formål og avtale. e) Alle testkontoer som er tildelt testbrukere skal deaktiveres. Testkontoene bør ikke slettes før de ikke lenger er nødvendig for å kunne spore testbrukerens aktivitet.[42] f) Test som utføres på en kopi av reelle data utløser krav om innsynslogg der pasienten skal kunne be om å denne utlevert, på samme måte som produksjon.

[39] F.eks. Microsoft, Cisco o.l. tester gjennomfører normalt grundige funksjonelle og sikkerhetsmessige tester av produkter eller oppdateringer slippes på markedet.
[40] Normen 6.0 kapittel 5.4.1 (andre ledd)
[41] Normen 6.0 kapittel 5.4.2.
[42] Se NSMs grunnprinsipper for IKT-sikkerhet 2.6.2