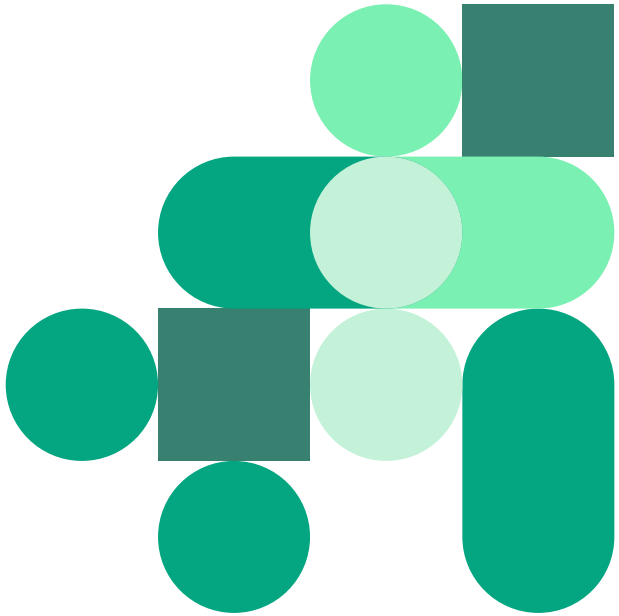
Underlag til Produkstyret

ROS verifikasjon i produksjon

Norsk helsenett

Risikoscenarioer



Scenario A

Feil blir ikke avdekket før produksjonssetting

Produksjonsmiljøet er et separat og unikt miljø med særskilte problemstillinger som ikke nødvendigvis er tilstede i testmiljøet (f. eks andre integrasjoner, kommunikasjonsflyt og adresser). Ikke produksjonsnære testmiljøer kan føre til at det produksjonsettes feil som oppstår eller blir synlige ved overgang fra testmiljøet til produksjonsmiljøet. I tillegg er overgangen til produksjonsmiljøet en manuell prosess for mange av helseforetakene.

Feil i løsningene kan innebære at innbyggere ikke får tilgang til meldinger eller innsyn de skulle ha hatt, og/eller at innbygger får meldinger eller innsyn de ikke skulle hatt.

Dette fører til risiko for at innbygger/pasient ikke får nødvendig helsehjelp, og kan føre til omdømmetap/tillitstap mot helsevesenet dersom data kommer på avveie.

Dette kan videre innebære regelverksbrudd med varsel eller vedtak, og som ytterste konsekvens risiko for liv og helse. Konsekvens kan også være at man velger å ikke produksjonsette nye løsninger eller skru av eksisterende tjenester grunnet for stor usikkerhet knyttet til overgang fra testmiljø til produksjonsmiljø.

Scenario B

Ansattes helsejournal inneholder uriktig data

Ved produksjonsetting av endringer og i tilfeller når feil i produksjonsmiljøet ikke lar seg gjenskape i testmiljøet, øker det behovet for å gjennomføre verifikasjon i produksjon hos helseforetakene. Dette kan være resultat av kompleksiteten knyttet til produksjonsmiljøet og at testmiljøene ikke er tilstrekkelige.

Dette medfører at ansatte føler seg presset til å bruke egen BankID for innlogging, samt egen pasientjournal for å verifisere at endringer og tjenester fungerer i produksjonsmiljøet på Helsenorge.

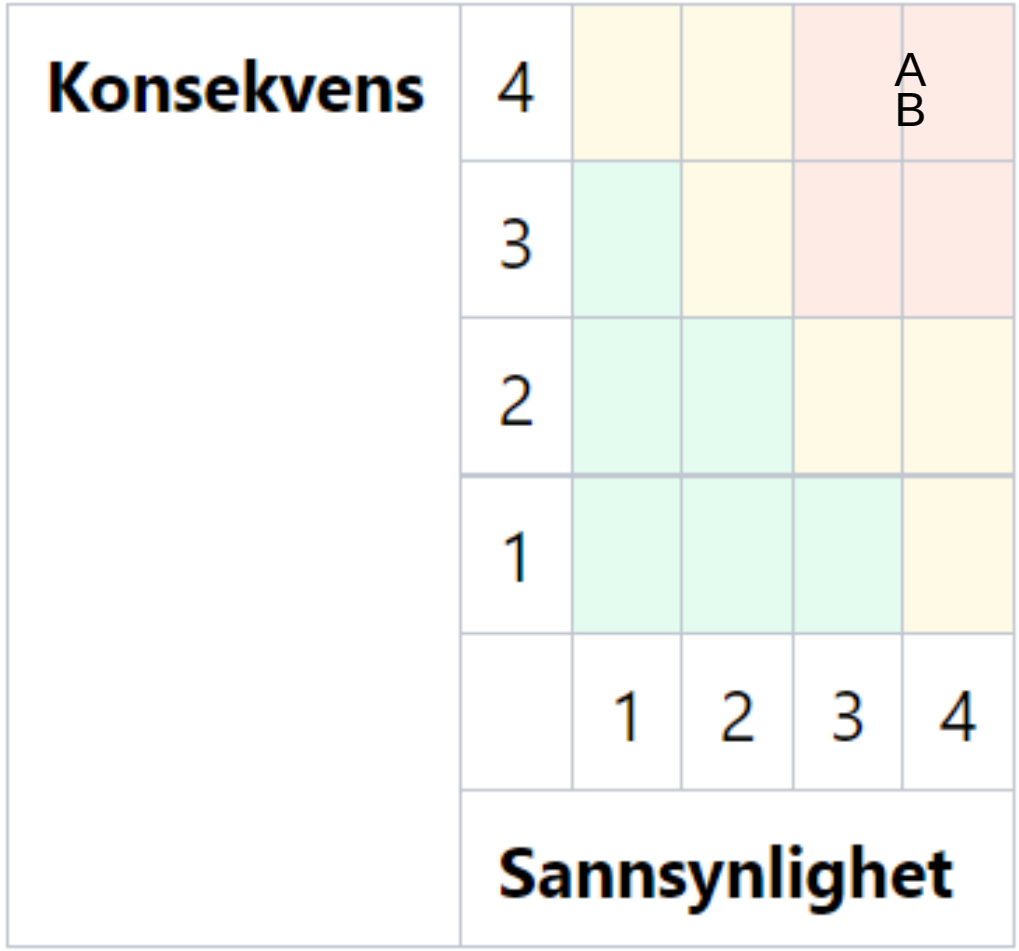
Som en konsekvens kan ansattes pasientjournaler inneholde falske (uriktige) data om deres helseforhold. Dette kan utilsiktet føre til feilbehandling fordi pasientjournalen ikke inneholder korrekt data om ansattes helseforhold. I ytterste konsekvens setter dette ansattes liv og helse i fare.

I tillegg vil dagens praksis medføre regelverksbrudd, som kan føre til blant annet formelle advarsler, bøter eller vedtak til NHN og helseforetakene.

Vurdering av sannsynlighet og konsekvens

Risiko scenario A og B

Risikomatrise før tiltak



Tabell for vurdering av sannsynlighet

Kriterier for valg av sannsynlighet			
Verdi	**Beskrivelse**	**Erfaring/Trend?**	**Beskrivelse letthet**
4	**Meget sannsynlig**	Har skjedd hos oss og andre.	• Sikkerhet er ikke etablert. • Krever små til normale ressurser av egne medarbeidere eller eksterne for å brytes. • Ikke nødvendig med kjennskap til tiltakene. • Sikkerhetstiltak er sterkt avhengig av at en eller flere manuelle rutiner/policyer følges
3	**Sannsynlig**	Har hørt om hos andre, kunne like gjerne vært hos oss.	• Sikkerhetstiltak er ikke fullt etablert i forhold til sikkerhetsbehovet. • Sikkerhetstiltak fungerer ikke etter hensikten. • Egne medarbeidere trenger kun små til normale ressurser for å bryte tiltakene. • Eksterne trenger små/normale ressurser og normal kjennskap til tiltakene for å bryte disse.
2	**Mindre sannsynlig**	Har hørt om, men aldri hos oss.	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet. • Sikkerhetstiltak fungerer etter hensikten. • Egne medarbeidere trenger små til normale ressurser og normal kjennskap til tiltakene for å bryte disse. • Eksterne trenger gode ressurser og god kjennskap til tiltakene for å bryte disse.
1	**Lite sannsynlig**	Har aldri hørt om.	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet. • Sikkerhetstiltak fungerer etter hensikten. • Krever gode ressurser og godt kjennskap av egne medarbeidere for å brytes. • Eksterne kan ikke omgå tiltakene.

Tabell for vurdering av konsekvens (del 1)

Kriterier for valg av konsekvens							
Verdi	**Beskr.**	**Personvern**	**Liv og helse** (Berører hvor mange?)	**Regelverk**	**Tjenesteytelse og tidsaspekt i forhold til tjenestekritikalitet** Ute av drift /redusert kvalitet	**Omdømme**	**Økonomi**
4	**Meget stor**	Langvarig tap av anseelse eller personlig integritet • Inngripende personopplysninger om mange personer • Fortrolig eller strengt fortrolig informasjon om mange personer • Særlig kategori personopplysninger om mange personer • Den registrertes rettigheter og personvernprinsippene er ikke ivaretatt	Dødsfall eller alvorlige personskader (flere personer) på grunn av mangel eller feil hos NHN eller underleverandører.	Regelverksbrudd som medfører vedtak, foretaksstraff/bøter og/eller fengselsstraff.	• System som benyttes av alle virksomheter og/eller har stor betydning er midlertidig ute av drift eller redusert. • Stopp/reduksjon omhandler alle brukere. • Personsensitiv informasjon kan ha gått tapt eller kan ikke stoles på.	Vesentlig tap av tillit hos brukere/kunder, eier og andre viktige interessenter. Omfattende og svært negative oppslag i media (redaksjonelle medier og sosiale medier).	Tap på over 50 mill. kroner
3	**Stor**	Tap av anseelse eller personlig integritet som er krenkende • Inngripende personopplysninger om flere personer / eller lite inngripende personopplysninger om mange personer • Fortrolig eller strengt fortrolig informasjon om en eller få personer • Særlig kategori personopplysninger om en eller få personer	Alvorlig personskade (én person) på grunn av mangel eller feil hos NHN eller underleverandører.	Regelverksbrudd som medfører advarsel eller vedtak, samt mulig foretaksstraff/bøter.	• System av stor utbredelse/betydning er midlertidig ute av drift eller redusert. • Stopp/reduksjon som omhandler de fleste brukerne. • Virksomhetskritisk informasjon kan ha gått tapt eller kan ikke stoles på.	Tap av tillit hos brukere/kunder, eier og andre viktige interessenter. Negative oppslag i media over flere dager.	Tap mellom 15 og 50 mill.

Tabell for vurdering av konsekvens (del 2)

Kriterier for valg av konsekvens							
Verdi	**Beskr.**	**Personvern**	**Liv og helse** (Berører hvor mange?)	**Regelverk**	**Tjenesteytelse og tidsaspekt i forhold til tjenestekritikalitet** Ute av drift /redusert kvalitet	**Omdømme**	**Økonomi**
2	**Mindre**	Tap av anseelse eller personlig integritet som kan oppfattes som krenkende • Lite inngripende personopplysninger om flere personer • Ingen fortrolig eller strengt fortrolig informasjon • Ingen særlig kategori personopplysninger • Den registrertes rettigheter og personvernprinsippene er i det vesentlige ivaretatt	Mindre alvorlig personskade på grunn av mangel eller feil hos NHN eller underleverandører.	Regelverksbrudd som kan medføre advarsel eller vedtak.	• System av større utbredelse/betydning er midlertidig ute av drift eller redusert. • Stopp/reduksjon som omhandler noen brukere. • Informasjon unntatt offentlighetsloven kan ha gått tapt eller kan ikke stoles på.	Mindre eller kortvarige oppslag i media som kan ved gjentatte tilfeller føre til tap av tillit.	Tap mellom 3 og 15 mill.
1	**Liten**	Ubetydelig tap av anseelse eller personlig integritet • Lite inngripende personopplysninger om få personer • Ingen fortrolig eller strengt fortrolig informasjon • Ingen særlig kategori personopplysninger	Ubetydelig personskade på grunn av mangel eller feil hos NHN eller underleverandører.	Ubetydelig regelverksbrudd.	• System av mindre utbredelse/betydning er midlertidig ute av drift er midlertidig ute av drift eller redusert. • Stopp/reduksjon som omhandler få brukere. • Åpen/tilgjengelig informasjon kan ha gått tapt eller kan ikke stoles på.	Henvendelse fra media uten negative oppslag.	Tap mellom 500.000 og 3 mill.

Tiltak identifisert i workshoper med RHF’ene mappet mot delscenarioer

Feil blir ikke avdekket før produksjonssetting

Delscenario A

Produksjonsmiljøet er et separat og unikt miljø med særskilte problemstillinger som ikke nødvendigvis er tilstede i testmiljøet (f. eks andre integrasjoner, kommunikasjonsflyt og adresser).

Ikke tilstrekkelig produksjonsnære testmiljøer kan føre til at det produksjonsettes løsninger som oppstår eller blir synlige ved overgang fra testmiljøet til produksjonsmiljøet

Tiltak

- Syntetiske testbrukere med BankID i produksjonsmiljøet
- Bedre overvåking av produksjonsmiljø, spesielt ved produksjonssetting
- Etablere nødvendige testmiljøer
- Økte ressurser til testmiljøene (både antall ansatte og mer midler)
- Økt kompetanse og kapabiliteter for testing
- Helhetlig arkitekturskisser for hele verdikjeden
- Sårbarhetsmodellering for hele verdikjeden, f. eks gjennom OWASP SAMM

Feil blir ikke avdekket før produksjonssetting

Delscenario A

I tillegg er overgangen til produksjonsmiljøet en manuell prosess for mange av helseforetakene.

Tiltak

- Bruke "Fire øyne" (en person gjør jobben og en person kontrollerer) for å redusere risikoen for manuelle feil ved produksjonssetting
- Rigg for automatiserte tester slik at feil ved manuelle endringer avdekkes
- Automatisering/mindre manuell konfigurering i produksjonssettingen
- Automatiserte tester som dekker hele verdikjeden i testmiljø

Feil blir ikke avdekket før produksjonssetting

Delscenario A

Feil i løsningene kan innebære at innbyggere ikke får tilgang til meldinger eller innsyn de skulle ha hatt, og/eller at innbygger får meldinger eller innsyn de ikke skulle hatt.

Dette fører til risiko for at innbygger/pasient ikke får nødvendig helsehjelp, og kan føre til omdømmetap/tillitstap mot helsevesenet dersom data kommer på avveie.

Tiltak

- Bedre beskrivelser på endringer som treffer HF'ene (inkl. hotfixer), f. eks er «tekniske forbedringer» for lite detaljert.
- Bruke pilotgruppe for validering i stedet for egen BankID/journal (f. eks bruke en avdeling eller ringe enkeltpasienter for å høre om de har mottatt brev osv.)
- Informasjon om bruk av syntetisk data, f. eks hvordan er dataflyten mot andre testdatabaser i verdikjeden
- Bedre loggdata, samt rutinemessig logganalyse og logg-gjennomgang

Feil blir ikke avdekket før produksjonssetting

Delscenario A

Dette kan videre innebære regelverksbrudd med varsel eller vedtak, og som ytterste konsekvens risiko for liv og helse.

Konsekvens kan også være at man velger å ikke produksjonsette nye løsninger eller skru av eksisterende tjenester grunnet for stor usikkerhet knyttet til overgang fra testmiljø til produksjonsmiljø.

Tiltak

- Et grensesnitt for å sjekke status på tjenestene, f. eks for å overvåke at brevtjenesten fungerer som normalt.
- ROS-vurderinger av nye tjenester og endringer før produksjonssetting

Ansattes helsejournal inneholder uriktig data

Delscenario B

Ved produksjonsetting av endringer og i tilfeller når feil i produksjonsmiljøet ikke lar seg gjenskape i testmiljøet, øker det behovet for å gjennomføre verifikasjon i produksjon hos helseforetakene.

Dette kan være resultat av kompleksiteten knyttet til produksjonsmiljøet og at testmiljøene ikke er tilstrekkelige.

Tiltak

- Syntetiske testbrukere med BankID i produksjonsmiljøet
- Gode testscenarioer som er like i test og produksjon
- Bedre overvåking av produksjonsmiljø, spesielt ved produksjonssetting
- Etablere nødvendige testmiljøer
- Økte ressurser til testmiljøene (både antall ansatte og mer midler)
- Økt kompetanse og kapabiliteter for testing
- Helhetlig arkitekturskisser for hele verdikjeden
- Sårbarhetsmodellering for hele verdikjeden, f. eks gjennom OWASP SAMM

Ansattes helsejournal inneholder uriktig data

Delscenario B

Dette medfører at ansatte føler seg presset til å bruke egen BankID for innlogging, samt egen pasientjournal for å verifisere at endringer og tjenester fungerer i produksjonsmiljøet på Helsenorge.

Tiltak

- Bedre beskrivelser på endringer som treffer HF’ene (inkl. hotfixer), f. eks er «tekniske forbedringer» for lite detaljert.
- Bruke pilotgruppe for validering i stedet for egen BankID/journal (f. eks bruke en avdeling eller ringe enkeltpasienter for å høre om de har mottatt brev osv.)
- Informasjon om bruk av syntetisk data, f. eks hvordan er dataflyten mot andre testdatabaser i verdikjeden
- Bedre loggdata, samt rutinemessig logganalyse og logg-gjennomgang

Ansattes helsejournal inneholder uriktig data

Delscenario B

Som en konsekvens kan ansattes pasientjournaler inneholde falske (uriktige) data om deres helseforhold. Dette kan utilsiktet føre til feilbehandling fordi pasientjournalen ikke inneholder korrekt data om ansattes helseforhold. I ytterste konsekvens setter dette ansattes liv og helse i fare.

I tillegg vil dagens praksis medføre regelverksbrudd, som kan føre til blant annet formelle advarsler, bøter eller vedtak til NHN og helseforetakene.

Tiltak

- Gode prosedyrer på hva som er tillatt og ikke tillatt i produksjonsmiljø
- Loggføre og dokumentere når ansatte bruker egne data (BankID) til å verifisere i produksjon på Helsenorge

Tiltak identifisert i workshoper med RHF’ene – oppsummert

Innspill fra workshopene (ikke rangert rekkefølge)

Ansvar: NHN

Ønsket tiltak fra RHF (kortsiktige tiltak)	Kommentarer
Syntetiske testbrukere med BankID i produksjonsmiljøet,	NHN: Skatteetaten har avvist NHN sin forespørsel
Testbrukere som ikke trenger BankID for å verifisere i produksjon / Fullmakt til ansatte (testere) for å få bruke testaktører (syntetiske identiteter i produksjonsmiljøet)	RHF: Ønsker at NHN utreder av dette, kan f. eks bruke hvitelisting.
Sertifiseringsordning for tjenester som produksjonssettes. En aktør som sertifiserer tjenesten på nytt ved endringer. Utfordre NHN til å undersøke dette nærmere. Noen land har etablert en slik løsning.	RHF: Ønsker at NHN utreder dette.
Et grensesnitt for å sjekke status på tjenestene, f. eks for å overvåke at brevtjenesten fungerer som normalt.	NHN undersøker behovet og muligheten for dette nærmere.
Bedre beskrivelser på endringer som treffer HF'ene (inkl. hotfixer), f. eks er «tekniske forbedringer» for lite detaljert.	NHN undersøker hvilke beskrivelser dette gjelder, og hva som kan gjøres for å legge til rette for rett detaljeringsnivå for RHF'ene.
Informasjon om bruk av syntetisk data, f. eks hvordan er dataflyten mot andre testdatabaser i verdikjeden	NHN kan legge til rette for deling av informasjon og kompetanse om bruk av syntetiske data.
Helhetlig arkitekturskisser for hele verdikjeden	Det finnes ende-til-ende skisser på noen tjenester, men ikke på alle. NHN kan tilrettelegge for at RHF'ene får tilgang på beskrivelser av alle tjenestene på Helsenorge.
Sårbarhetsmodellering for hele verdikjeden, f. eks gjennom OWASP SAMM	NHN har et pågående prosjekt med HSØ/SP
Automatiserte tester som dekker hele verdikjeden i testmiljø	NHN benytter automatiserte tester, dette kan utvides til verdikjeden

Innspill fra workshopene (ikke rangert rekkefølge)

Ansvar: RHF

Tiltak:	Kommentar:
Bruke "Fire øyne" (en person gjør jobben og en person kontrollerer) for å redusere risikoen for manuelle feil ved produksjonssetting	
Etablere nødvendige testmiljøer	
Økte ressurser til testmiljøene (både antall ansatte og mer midler): Må ha mer midler.	
Økt kompetanse og kapabiliteter for testing	
Automatisering/mindre manuell konfigurering i produksjonssettingen	
Rigg for automatiserte tester slik at feil ved manuelle endringer avdekkes	
Bedre loggdata, samt rutinemessig logganalyse og logg-gjennomgang	
Gode prosedyrer på hva som er tillatt og ikke tillatt i produksjonsmiljø	
Bedre overvåking av produksjonsmiljø, spesielt ved produksjonssetting	
Gode testscenarioer som er like i test og produksjon	
Bruke pilotgruppe for validering i stedet for egen BankID/journal (f. eks bruke en avdeling eller ringe enkeltpasienter for å høre om de har mottatt brev osv.)	
Loggføre og dokumentere når ansatte bruker egne data (BankID) til å verifisere i produksjon på Helsenorge	
ROS-vurderinger av nye tjenester og endringer før produksjonssetting	

Forslag til beslutning

Det er ønskelig at alle aktører gjennomgår og kvalitetssikrer risikoscenarioene og tiltakene identifisert i workshopene i egen organisasjon, samt vurderer i hvilken grad tiltakene allerede er iverksatt eller må iverksettes. Merk at det kan finnes andre tiltak som ikke er identifisert.