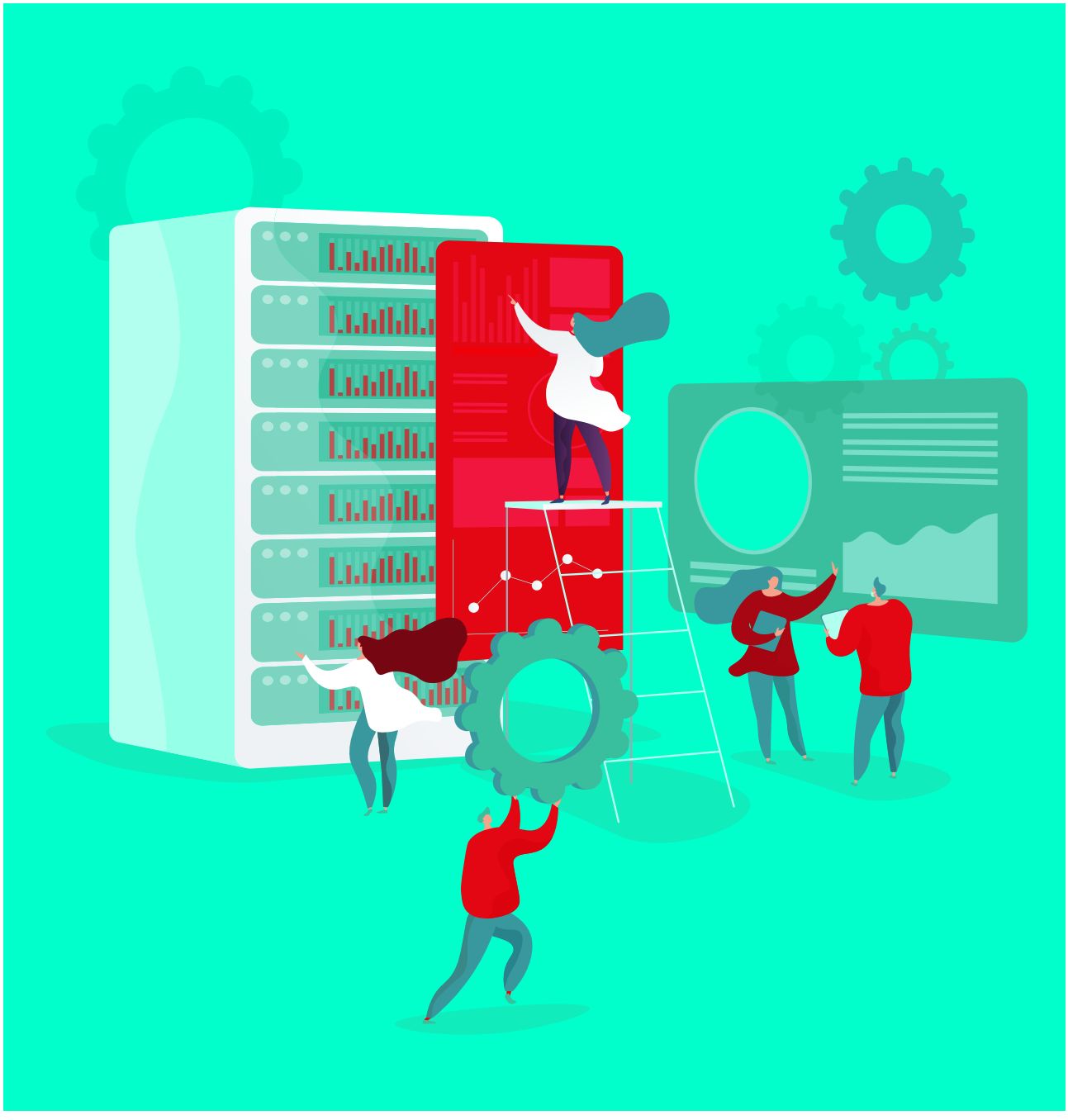
Risikovurderinger, nødrutiner og forbedringsarbeid ved 17 sykehus

# Forsvarlig pasient-behandling uten IKT?



Helsetilsynet
TILSYN MED BARNEVERN, SOSIAL- OG HELSETJENESTENE

RAPPORT 2/2021 • APRIL 2021

# Innhold

# Innhold

# Tabell- og figurregister

## Tabellregister



## Figurregister

# 1 Oppsummering

## 1.1 Hva gjorde vi?

Helsetilsynet har gjort en kartlegging av kritiske system, risikovurderinger og nødrutiner for IKT-system ved 17 virksomheter i spesialisthelsetjenesten. De fleste virksomhetene er offentlige helseforetak, men også to private ideelle sykehus har deltatt. Kartleggingen er videreføring av en undersøkelse som ble gjort ved fem virksomheter vinteren 2019/2020 (1).

Vi undersøkte i hvilken grad virksomhetene er forberedt på å håndtere situasjoner hvor kliniske IKT-system ikke er tilgjengelig. Vi har også sett på hvordan virksomhetene har identifisert og vurdert risiko knyttet til å kunne yte forsvarlig helsehjelp ved bortfall av IKT, og hvordan de har laget planer og tiltak basert på risikovurderingene. Vi har ikke gjort lovlighetskontroll av innsendte svar.

## 1.2 Hva fant vi?

### For svake nødrutiner og øvingsregimer for noen sentrale tekniske løsninger

Helseforetakene arbeider systematisk med å utarbeide nødrutiner og sørger for at helsepersonellet øver på å bruke de. Virksomhetene har imidlertid for svake nødrutiner og/eller øvingsregimer for noen tekniske løsninger som stans-, pasientalarmer og telefoni. Telefoniløsninger er sentrale i mange ordinære kritiske arbeidsprosesser, og de er sentrale i mange nødrutiner ved sykehusene. Samtidig baserer telefoniløsningene seg stadig mer på samme digitale nettverk som IKT-løsningene. Dermed vil disse kunne svikte samtidig som de andre IKT-løsningene. Det er derfor betenkelig at en stor del av virksomhetene ikke har øvd personell i bruk av nødrutiner for ulike telefoniløsninger eller lagd nødrutiner for eksempel for bruk av Nødnett ved bortfall av IKT. Dette er spesielt kritisk når andel angrep mot sykehus ser ut til å øke (2).

### Mangler systematisk oversikt over konsekvenser av IKT-bortfall for pasientsikkerhet

Funn i kartleggingen viser at virksomhetene har utarbeidet mange risikoanalyser for IKT-endringer. Men det er utarbeidet få overordnede risikovurderinger for bortfall av all IKT, noe som også er påpekt av Riksrevisjonen (3). De fleste risikoanalysene har fokus på tekniske forhold, og lite på konsekvenser av IKT-bortfall i klinisk virksomhet. Denne kartleggingen viser at helseforetakene også mangler systematisk oversikt over hvilke IKT-saker (feil- eller endringsønsker) som har størst konsekvens i forhold til forsvarlig helsehjelp og pasientsikkerhet. Ansvar for prioritering av IKT-saker knyttet til pasientsikkerhet er ›

«Kartleggingen avdekker manglende dataintegritet for viktig informasjon om pasientens legemiddelbruk.»

uklar flere steder, og helseforetakene mangler innsikt i hvilke IKT-saker som er meldt til regionale IKT-kundesenter. Uklare ansvarsforhold er en risiko i seg selv. Lovpålagt forbedringsarbeid blir vanskelig uten fullstendig informasjonsgrunnlag, organisering og støtteapparat rundt systemeiere. Virksomhetene undersøker ikke konsekvensene av å drive et sykehus uten IKT-støtte, og er ikke forberedte på å håndtere langvarige IKT-bortfall. Samtidig er mange av beredskapsepisodene i sykehus IKT-relaterte (4).

De regionale helseforetakene har plikt til å legge til rette for samarbeid, systematisk styring og forbedringer. Helseforetakene har ansvar for både informasjonssikkerhet og risikovurderinger knyttet til forsvarlig helsehjelp (5). Krav til konfidensialitet, personvern og tilgjengelighet er håndfaste og målbare. Tilfredsstillende brukervennlighet, dataintegritet (samsvarende/ oppdatert informasjon i ulike system), forsvarlige funksjoner og opplæring lar seg ikke like enkelt spesifisere, og vurdering av kliniske risikoer krever helsefaglig kompetanse. De fleste innsendte risikoanalysene er svake på disse områdene.

IKT-feil og endringsønsker meldes til IKT-kundesenter. Avvik i pasientbehandlingen skal meldes i det interne avvikssystemet i helseforetaket. Dermed må helsepersonell registrere IKT-saker som fører til avvik i pasientbehandlingen to steder. Dette er utfordrende på flere måter. NPE finner også at bare 33 % av sakene som har fått medhold om pasientskadeerstatning, er meldt i sykehusenes egne avvikssystem (6).

**Dårlig oversikt over gjeldende legemiddelbruk fordi like data lagres i flere IKT-systemer uten konsistenssjekk**

I to regioner har helseforetakene oppgitt at IKT-driftsleverandører har ansvar for risikovurderinger knyttet til total informasjonssikkerhet (tilgjengelighet, integritet og konfidensialitet). Helsetilsynet ser svakheter ved å skille mellom ansvar for datakonsistens og forsvarlig helsehjelp. Det er uheldig at det brukes ulike definisjoner for informasjonssikkerhet i sektoren, der perspektivet med datakonsistens/ dataintegritet (7) i mange sammenhenger faller bort. Tilgang til riktige data er en forutsetning for å levere forsvarlige helsetjenester. Kartleggingen avdekker manglende intern dataintegritet for viktig informasjon om pasientens legemiddelbruk. Til tross for kjente utfordringer med legemiddelinformasjon og visjon om «Én innbygger - én journal» (8) er det i mange virksomheter innført nye system med duplikate data, krav til ekstra pålogging og ekstra oppslag (pasientsøk) for helsepersonell. Praksisen med slik dokumentasjon i flere system strider mot kravet om at journalen skal gi en samlet framstilling av pasientens helsetilstand. ›

> «Få eller ingen virksomheter har tilgang til pasientinformasjon om nye pasienter dersom sentral journaldatabase feiler.»

Elektroniske medikamentkurver er under innføring ved alle helseforetak i spesialisthelsetjenesten. Disse systemene er svært sentrale verktøy i kliniske avdelinger og løsningene medfører økt sårbarhet ved tekniske feil. En stor del av helseforetakene med elektronisk medikamentkurve svarer at nødrutinen for medikamentutdeling bare delvis sikrer forsvarlig legemiddelutdeling.

**Dersom helseopplysninger ikke er tilgjengelige kan det forårsake pasientskader**

Risikoen for helsesvikt øker jo lenger IKT-bortfall varer, hvor akutt syk pasienten er og hvor ukjent sykehistorien er for behandler. Flertallet av virksomhetene vurderer at det blir vesentlig risiko for svikt i helsetjenester etter mindre enn 2 timer når EPJ-system (DIPS/ DocuLive) faller bort. Bare to helseforetak har nødrutiner som sikrer at de har tilgang til journalinformasjon for nye pasienter dersom nettverksfeil hindrer forbindelse til EPJ-database. Få eller ingen virksomheter har tilgang til pasientinformasjon om nye pasienter dersom sentral journaldatabase feiler. Manglende tilgang til EPJ ved akuttmottak utgjør en risiko for pasientsikkerheten. Ved bortfall av IKT mister dessuten sykehusene etter kort tid oversikt over inneliggende pasienter.

Kartleggingen viser at IKT-feil kan slå ut system for prioritering av pasienter og koordinering av ambulanser ved alle sykehus i en region samtidig. Ingen foretak har samarbeidsavtale med AMK-sentral (akuttmedisinsk kommunikasjonssentral) i annen region.

**Personvernhensyn vektes ikke mot krav til forsvarlig helsehjelp**

Noen virksomheter melder det som utfordrende å lage gode beredskapsløsninger som tilfredsstiller både personvern og forsvarlig helsehjelp. Risikovurderingene av personvern og pasientsikkerhet bør i større grad vektes mot hverandre, og det må planlegges for løsninger som tilfredsstiller begge krav.

Risikoanalyser av e-konsultasjoner som en metode for å gi forsvarlig helsehjelp, er bare gjort ved et par helseforetak. Alle har vurdert personvernaspektet av metoden. For å redusere smitte er det fornuftig for helseforetak å vekte risiko for smitte ved fysiske møter større enn annen risiko for svikt ved videokonsultasjon i helsetjenesten når en ny og ukjent pandemi inntreffer. Etter hvert bør en utarbeide risikoanalyser, løsninger og kliniske retningslinjer for bruk av e-konsultasjoner som ivaretar begge aspekter. ›

## 1.3 Behov for forbedringer

**Alle virksomheter må:**

- utarbeide overordnede risikoanalyser som tar med konsekvenser for helsehjelp ved IKT-bortfall. Helsepersonell må delta i utredning av konsekvenser og utarbeiding av tiltak. Risikoanalysene og tilhørende tiltak må vurderes av foretaksledelsen.
- vurdere tiltak for å sikre tilgang til journalinformasjon for nye pasienter ved bortfall av EPJ, og vurdere lignende backupløsninger for nøkkelpersonell som koordinatorer i sentraloperasjoner eller lignende
- utarbeide tidfestede planer for å oppnå dataintegritet (riktig informasjon i ulike system) for legemiddeldata og annen kritisk informasjon (informasjon som i en behandlingssituasjon kan medføre at planlagte tiltak endres, og kanskje redder pasientens liv eller forhindrer alvorlig skade)
- gjennomgå og teste nødrutiner for bortfall av ordinære kommunikasjonskanaler som forutsetter IKT-nettverk eller ordinære telefonsamband
- ha en oppdatert oversikt over de IKT-saker (feil og endringsønsker) som har størst risiko når det gjelder forsvarlig helsehjelp, og benytte dette i kontinuerlig forbedringsarbeid. Slike data må kunne hentes både fra interne avvikssystem i helseforetakene og fra IKT-driftsleverandørens kundesentersystem. Helseregionene må organiseres slik at virksomhetene kan arbeide systematisk og helhetlig med å gjøre IKT-løsningene forsvarlige for pasientbehandlingen. Dette vil kreve klinisk involvering, et kompetent støtteapparat rundt systemeiere og tydelig ansvarsplassering i alle ledd fra innkjøp til avvikling.

**Noen virksomheter:**

- må utbedre nødrutiner for å holde oversikt over pasienter ved IKT-bortfall
- må sikre oppdatert legemiddelinformasjon ved ev. bortfall av elektronisk legemiddelkurve
- må oppdatere sine lister over kritiske system i Helse Vest (utført 1.1.21 red.anm.)
- bør sikre tilgang til Kjernejournal ved bortfall av EPJ, eksempelvis via elektronisk kurve eller AMIS (der API er utviklet)
- må sikre at innbyggerne har tilgang til medisinsk nødmeldings- og kommunikasjonstjeneste via nødnummer 113, også ved stor ›

belastning på telefon og omfattende IKT-hendelser. Dette kan for eksempel gjøres ved at noen virksomheter inngår samarbeidsavtaler med andre helseregioner.

- må etablere rutine for øvelser på nødrutine for bortfall av kritiske system som telefoni, stans- eller sykesignalsystem
- må sikre tilstrekkelig varsling til samarbeidende virksomheter ved planlagt og ikke-planlagte IKT-bortfall dersom de kun har elektroniske henvisninger ●

# 2 Bakgrunn og metode

## 2.1 Lovgrunnlag

Helsetjenester som tilbys eller ytes skal være forsvarlige, jf. spesialisthelsetjenesteloven § 2-2. Forsvarlighetskravet er en rettslig standard, som blant annet er forankret i anerkjent fagkunnskap, faglige retningslinjer og allmenngyldige samfunnsetiske normer. Virksomheter har videre en plikt til å sørge for at journal- og informasjonssystemene er forsvarlige.

Helsetjenesten er gjennom sin styring pålagt å sikre forsvarlige tjenester. Det følger av forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten at virksomheten har en plikt til å planlegge, gjennomføre, evaluere og korrigere sin virksomhet.

Virksomheten må kunne gi nødvendige tjenester også ved hendelser som truer virksomhetens drift eller som krever økt kapasitet. Virksomhetenes forpliktelse til å utarbeide og vedlikeholde egne beredskapsplaner fremgår av helseberedskapsloven. Forskrift om krav til og organisering av kommunal legevaktordning, ambulansetjeneste, medisinsk nødmeldetjeneste har også spesifikke krav til IKT-beredskap.

Det følger av helsetilsynsloven at Statens helsetilsyn har myndighet til å føre tilsyn med om tjenestene er i samsvar med det som er bestemt i lover og forskrifter.

> «Å kunne yte forsvarlig helsehjelp av god kvalitet er nært forbundet med brukervennlige og sikre IKT-verktøy som legger til rette for digital samhandling og skaper sammenheng mellom de ulike nivåene i tjenesten.»

## 2.2 Utviklingstrender

Det er i dag vanskelig å tenke seg forsvarlig drift av sykehus uten omfattende bruk av ulike IKT-system. Å kunne yte forsvarlig helsehjelp av god kvalitet er nært forbundet med brukervennlige og sikre IKT-verktøy som legger til rette for digital samhandling og skaper sammenheng mellom de ulike nivåene i tjenesten.

Koronapandemien har medført et taktskifte i digitaliseringen av helsetjenesten, og digitaliseringen er en ønsket utvikling (9).

Den omfattende digitaliseringen i helsevesenet krever et økt fokus på informasjonssikkerhet og brukervennlighet i løsningene. IKT-systemer er etter hvert blitt viktige forutsetninger for helsetjenestens evne til å yte forsvarlig helsehjelp. I den digitale helsetjenesten henger brukervennlighet, kvalitetsarbeid og pasientsikkerhet nøye sammen. Det er klare føringer fra regjeringen om å øke oppmerksomhet om kvalitet og pasientsikkerhet (10).

Det er stor variasjon i måten tjenesten har organisert sin IKT-drift på. Dette medfører ulike valg av sourcingstrategier (11). Et felles utviklingstrekk er at drift av IKT-løsninger sentraliseres i forsøk på å tilby mer effektive og robuste tjenester med forbedret oppetid og ›

sikkerhet. Imidlertid kan sentralisering føre til andre sårbarheter, som at konsekvensen av feil og mangler ved IKT-systemene blir større, fordi de affiserer systemer ved flere foretak samtidig. Sentralisering kan utfordre styringsmodeller og skape uklarhet rundt roller, ansvar og oppgaver for sikker drift av IKT-systemene.

Alle virksomhetene i denne kartleggingen benytter én regionsintern hovedleverandør av IKT-tjenester, unntatt ett privat ideelt foretak med egen IKT-driftsavdeling. Hovedleverandørene av IKT-tjenestene, IKT-driftsleverandørene, eies av de overordnede RHF-ene. IKT-driftsleverandørene leverer IKT-tjenester som blant annet infrastruktur, maskinvare, utvikling, innkjøp, forvaltning av programvare og tilgangsstyring. Både IKT-driftsleverandørene og sykehusene oppgir at de også kjøper IKT-tjenester som for eksempel telefonitjenester fra andre leverandører.

Fremover forventer vi å se økt bruk av løsninger som elektronisk kurve, sensorteknologi, avstandsoppfølging, automatisk datafangst fra medisinsk teknisk utstyr, beslutningsstøtte og kunstig intelligens (12). Helsehjelp vil understøttes av IKT-verktøy i økende grad. Dette medfører store endringer i måten helsepersonell arbeider på og hvordan virksomhetene organiserer sin aktivitet. Digitaliseringen av helsevesenet utfordrer også virksomhetene i hvordan de både sikrer persondata og andre data av verdi (7).

Forsvarlig helsehjelp vil i stadig større grad hvile på bruk av ulike tekniske løsninger. Pasientsikkerheten i sykehus skal være ivaretatt også når ett eller flere IKT-system er utilgjengelige. Formålet med kartleggingen er å bidra til læring, slik at virksomhetene kan yte forsvarlig helsehjelp, også ved bortfall av IKT.

## 2.3 Metode og antall besvarelser

Denne kartleggingen er utført ved 17 virksomheter, der 15 virksomheter er offentlige helseforetak og to virksomheter er private ideelle sykehus. Hver virksomhet pekte ut kontaktperson for kartleggingen. De fleste kontaktpersonene var IKT-ledere, rådgivere eller informasjonssikkerhetsledere i e-helseavdelinger i virksomhetene. Ved et helseforetak var fagdirektør kontaktperson for kartleggingen. Kontaktpersonene svarte på elektroniske spørsmål og sendte inn vedlegg fra 26.6 til 6.9.2020. Deretter deltok de i møter for å avklare spørsmål og uklarheter. Det er gjennomført elektroniske møter med alle virksomhetene for å oppklare eventuelle uklarheter. De fleste møtene er gjennomført som fellesmøter der vi har samlet flere foretak fra samme helseregion. ›

«Gjennom oppfølgingssamtaler har deltakerne gitt tilbakemeldinger om at kartleggingen har hatt verdi for dem. Noen foretak har begynt arbeidet med å vurdere kliniske konsekvenser ved langvarige IKT-bortfall.»

Kartleggingen bygger på en tidligere kartlegging som ble gjort ved fem virksomheter våren 2020 (1). Alle helseforetak og private sykehus som har akuttfunksjoner (øyeblikkelig hjelp) er undersøkt i disse to kartleggingene.

I denne andre kartleggingen ble det sendt ut 69 spørsmål til hver av virksomhetene (vedlegg 3). For en del tema er virksomhetene bedt om å besvare spørsmål med innsending av vedlegg. Helsetilsynet har samlet tatt imot cirka 350 dokumenter fra virksomhetene i denne siste kartleggingen. En del virksomheter har også innhentet og videresendt dokumentasjon fra regionale IKT-driftsleverandører.

Vi ville undersøke i hvilken grad virksomhetene er forberedt på å håndtere situasjoner med bortfall av IKT-systemer. Under dette ville vi også se på hvordan virksomhetene har vurdert risiko knyttet til å kunne yte forsvarlig helsehjelp ved bortfall av IKT, har fulgt opp avviksrapporter og hvordan de har utviklet og implementert planer og tiltak basert på vurderingene. Helsetilsynet har ikke gjort en lovlighetskontroll av innsendte svar. Innsendte svar og forslag til læring er i all hovedsak vurdert ut fra hvilke konsekvenser bortfall av kritiske IKT-systemer vil få for forsvarlig helsehjelp og pasientsikkerhet. Det følger av dette at i den grad informasjonssikkerhet (7) er vurdert, er det i all hovedsak lagt vekt på tilgjengelighet og i noen grad integritet. Helsetilsynet har valgt å bruke følgende definisjon på dataintegritet: «Integritet innebærer at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig og et resultat av autoriserte og kontrollerte aktiviteter.» (7).

Kvaliteten på nødrutinene er ikke vurdert i detalj. Det er innhentet et utvalg av risikoanalyser fra virksomhetene. Basert på funnene fra kartleggingen kan det bli aktuelt å vurdere andre former for kartlegginger/tilsynsaktiviteter. Kartleggingen inkluderer ikke tiltak hos IKT-driftsleverandører for å redusere risiko for IKT-bortfall.

Gjennom oppfølgingssamtaler har deltakerne gitt tilbakemeldinger om at kartleggingen har hatt verdi for dem. Noen foretak har begynt arbeidet med å vurdere kliniske konsekvenser ved langvarige IKT-bortfall. ●

# 3 Besvarelser, faktum og refleksjoner

## 3.1 Hvilke IKT-system er viktigst for å kunne yte forsvarlig helsehjelp og sannsynligheten for at disse faller bort

### 3.1.1 Identifisering av kritiske systemer

Samtlige virksomheter oppgir at de har identifisert hvilke IKT-systemer som er mest kritiske, og som vil ha direkte konsekvenser for virksomhetens evne til å yte forsvarlig helsehjelp. 16 av 17 virksomheter (94 %) har sendt inn lister over de kritiske systemene de har identifisert.

Det er betydelig variasjon i både hvilke typer systemer virksomhetene vurderer som kritiske, samt i antall identifiserte systemer. Gjennomsnittet av antallet kritiske systemer er 22.

Helse Vest skiller seg ut ved at 4 av 5 virksomheter oppgir at kun 3-4 systemer er kritiske. Disse systemene er alle tilknyttet AMK. I møte med kontaktpersoner ble utvalg av kritiske system begrunnet med at IKT-driftsleverandøren ikke ønsket å ta med EPJ og kurvesystem, men at leverandøren i praksis følger opp EPJ og kurvesystem som kritiske.

De øvrige 12 virksomhetene (71 %) er mer samstemte i det de oppgir som kritiske systemer:

- EPJ (DIPS/DocuLive)
- Radiologisystemer (RIS/PACS)
- Elektronisk kurve (der det er innført)
- Medisinsktekniske systemer som pasientovervåkning
- Laboratoriesystemer
- Telefoni- og callingsystemer
- Byggtekniske systemer som adgangskontroll og alarmering

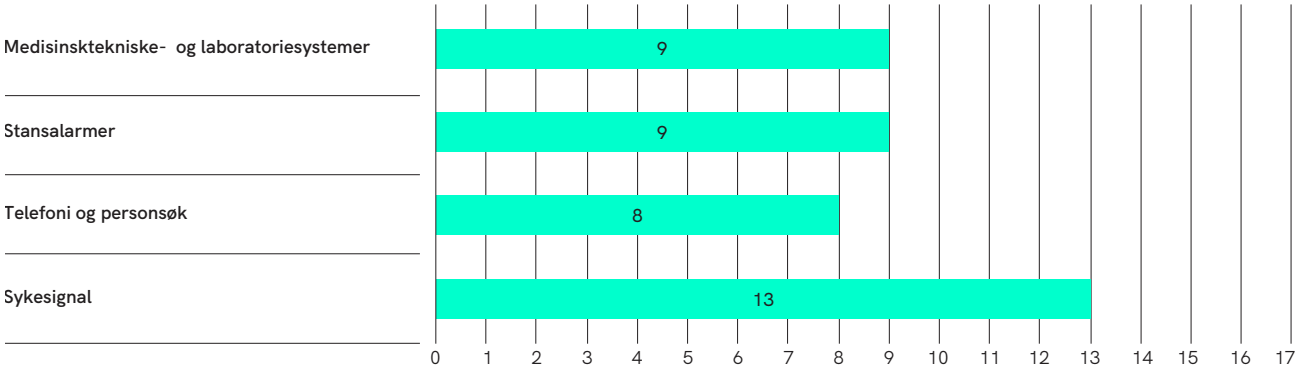
Vurderingen av hvilke systemer som er kritiske er forankret i virksomhetsledelsen ved alle foretak, og godkjent av administrerende direktør i ni virksomheter. I de resterende virksomhetene er godkjenningen gjort av medisinsk fagdirektør, IKT-leder eller andre med ansvarsroller i virksomhetsledelsen.

### 3.1.2 Hvilke system drifter virksomheten selv

Alle virksomhetene oppgir at de selv drifter IKT-systemer, i tillegg til driftstjenestene IKT-driftsleverandørene leverer. Det er betydelig variasjon i antallet systemer virksomhetene drifter selv, fra ett til flere ›

hundre. Virksomhetene oppgir at de for mange system deler på driftsoppgavene med IKT-leverandøren, for eksempel ved at IKT-driftsleverandøren leverer server og holder denne oppdatert med sikkerhetsoppdateringer. En virksomhet oppgir også å drifte en separat IKT-infrastruktur med serverrom, fysiske kabler, PC-er og strøm for sine tjenester. Dette kommer i tillegg til IKT-infrastrukturen som leveres av IKT-driftsleverandør.

*Figur 1 Antall virksomheter som har oppgitt å drifte denne typen system selv*




Figuren over viser system som helseforetak drifter selv. En del byggtekniske systemer som adgangskontroll, styring av ventilasjon og arealplanlegging kommer i tillegg.

Listen over laboratoriesystemer og systemer tilknyttet medisinsk utsyr er lang, men mange virksomheter oppgir samme type systemer:

- Spesialiserte PACS og radiologisystemer
- Pasientovervåkning
- Hjerteovervåkning/EKG
- EEG-systemer
- Øyesystemer
- Systemer tilknyttet de fleste laboratoriefunksjoner
- Brannvarsling

Systemene som foretakene selv har operativt driftsansvar for finnes også i listene over kritiske systemer. ›

> «Sannsynligheten for omfattende IKT-bortfall vurderes av to virksomheter til å være like høy som sannsynligheten for ekstremvær.»

### 3.1.3 Overordnede risikoanalyser og tilhørende nødrutiner

**Er en situasjon med bortfall av all IKT risikoanalysert?**
Deltakerne ble bedt om å svare på om bortfall av all IKT er risikovurdert, og de ble bedt om å sende inn risikovurderingene. Sju virksomheter svarer de har gjennomført en slik risikovurdering, sju svarer at de ikke har gjennomført dette. Tre svarer å ha delvis gjennomført en risikovurdering, men har ikke spesifisert hva dette innebærer.

15 av 17 virksomheter (88 %) har sendt inn vedlegg til spørsmålet, men det er variasjon i innholdet i vedleggene. Bare fire virksomheter har sendt inn risikoanalyser med risikomatriser. De øvrige innsendte dokumentene er sårbarhetsanalyser uten vurdering av konsekvens.

De fire innsendte risikoanalysene er utarbeidet av IKT-driftsleverandører og er teknisk detaljerte. Risikoanalysene inneholder lite detaljerte beskrivelser av konsekvensene av de identifiserte risikoene. Eksempler på oppgitte risikoer er tap av sentrale datarom, finansiering av WiFi, mangel på kompetanse, data- og virusangrep. Konsekvenser er vurdert på et overordnet nivå som at bortfall kan føre til forsinket diagnostikk og feilbehandling.

Et foretak har identifisert og analysert risiko for omfattende og langvarig IKT-bortfall, og satt opp tiltak for denne risikoen. Sannsynligheten for omfattende IKT-bortfall vurderes av to virksomheter til å være like høy som sannsynligheten for ekstremvær, og oppgis til å kunne skje inntil fire ganger i året.

Det er ikke vurdert grad av usikkerhet i risikovurderingene.

**Er det laget en egen nødrutine for bortfall av all IKT?**
I kartleggingen ba vi deltakerne svare på om de har utarbeidet nødrutiner for bortfall av all IKT, og eventuelt sende nødrutinene inn. 15 virksomheter har sendt inn i alt 63 vedlegg, der ti er beredskapsplaner (eller utdrag fra slike).

2 av virksomhetene (12 %) oppgir å ikke ha utarbeidet nødrutiner for bortfall av all IKT. 8 av 17 (47 %) svarer å ha dette, de resterende 7 (41 %) virksomhetene oppgir å delvis ha utarbeidet nødrutiner for bortfall av all IKT.

Innholdet i vedleggene som er sendt inn varierer fra å være foretaksovergripende nødrutiner for omfattende IKT-bortfall, nødrutiner for enkeltsystemer eller beredskapsplaner.

Nødrutinene for omfattende IKT-bortfall beskriver i stor grad overgang til manuelle rutiner og alternative kommunikasjonskanaler. ›

Samtlige virksomheter har foretaksovergripende nødrutiner for sentrale kliniske systemer som EPJ og radiologisystemer. 9 virksomheter (53 %) oppgir at klinikkene i tillegg er ansvarlige for å utarbeide lokale beredskapsplaner og nødrutiner for hendelser som kan påvirke klinikkenes evne til å yte helsehjelp.

**Øvelser**

På spørsmål om virksomhetene har testet nødrutine for bortfall av all IKT i øvelser svarer de:

| | |
|---|---|
| Testet i reell drift: | 8 |
| Ja, i øvelse: | 4 |
| Nei, ikke gjort øvelse: | 5 |

### 3.1.4 Øvrige risikoanalyser

Virksomhetene ble bedt om å sende inn oversikter over alle kjente IKT-endringer utført 2020 (med mulige konsekvenser for kliniske applikasjoner). Oversiktene viser:

16 av 17 virksomheter (94 %) svarer at det blir gjort risikoanalyser ved alle IKT-endringene som kan ha store konsekvenser for virksomhetene. 1 av 17 virksomheter (6 %) svarer at 'de ikke vet eller at det delvis utføres risikoanalyser' ved alle slike endringer.

På spørsmål om hvem som utfører risikoanalyser ved IKT-endringer kunne virksomhetene svare med flere alternativer.

*Tabell 1 Hvem utarbeider risikovurderinger?*

| | Svar | |
|---|---|---|
| Vi gjør egne risikovurderinger | 47,06 % | 8 |
| Vi gjør risikovurderinger sammen med IKT-driftsleverandøren | 64,71 % | 11 |
| IKT-driftsleverandøren gjør dette | 47,06 % | 8 |
| Varierende, ut fra situasjonen | 35,29 % | 6 |
| Det gjøres endringer uten kjent risiko | 5,88 % | 1 |
| Annet (vennligst spesifiser) | 23,53 % | 4 |
| **Totalt antall respondenter** | | **17** |

Virksomheter fra Helse Sør-Øst og Helse Midt-Norge har videresendt svar fra egne IKT-driftsleverandører. Der står det at IKT-leverandørene analyserer konfidensialitet, integritet, tilgjengelighet (samt sporbarhet ›

for Sør-Øst), og at helseforetakene må vurdere forsvarlig helsehjelp. Sitat fra Sykehuspartner:

«I spesifikasjonsfaser ved innføring av nye tjenester og anskaffelse av applikasjoner, legges grunnlaget for videre risikovurdering. Helseforetakene fastsetter hvor kritisk en IKT-tjeneste er for virksomheten og pasientbehandlingen (kritikalitet), og gjøre egne risikovurderinger bl.a. ut i fra konsekvenser for pasientsikkerhet, alternative reserveløsninger og nød-rutiner. Fastsetting av kritikalitet innebærer altså en risikovurdering i seg selv.

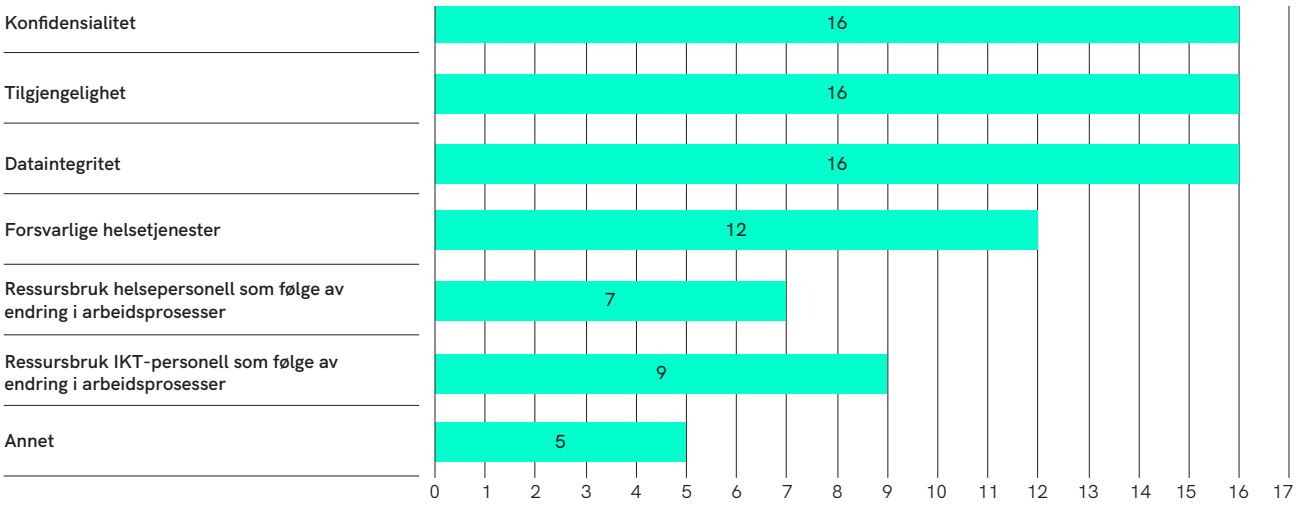
For medium og større IKT-endringer er det ofte behov for å utarbeide eller oppdatere et løsningsdesign. Designet er grunnlag for både implementering av tjenesten, samt å gjennomføre en risiko- og sårbarhetsvurdering (ROS). Den ROS-vurderingen omfatter konfidensialitet, integritet, tilgjengelighet og sporbarhet (KITS). Noen IKT-endringer er mer standardiserte og (f.eks. oppkopling av et standard MTU), og forenklede risikovurderinger kjøres.

Bestilte IKT-endringer fra helseforetakene til driftsleverandør Sykehuspartner utgjør en vesentlig andel av medium/store IKT-endringer, og styres nå gjennom årlig kundeplaner pr helseforetak. Informasjonssikkerhetsleder ved helseforetaket «eier» utarbeidede risikovurderinger, og avklarer om restrisiko etter evt beskrevne risikoreduserende tiltak er akseptabel for helseforetaket.

Det utarbeides i snitt over 30 slike ROS-vurderinger pr måned fra Sykehuspartner.»

Virksomhetene oppgir selv at følgende tema er vurdert i innsendte risikoanalyser ved oppgradering av kliniske system:

*Figur 2 Hvilke tema er vurdert i risikovurdering av oppgradering av klinisk system?*



Tilsvarende svar ble gitt på spørsmål om hvilke temaer som vanligvis risikovurderes ved endring av IKT-infrastruktur.

Innsendt materiale viser at risikoanalyser utføres i stort antall av både HF, IKT-driftsleverandører og andre som for eksempel regionale prosjekt. De fremstår i stor grad å være oppdaterte. Risikoanalysene som er sendt inn, er ikke enhetlige i form eller innhold. Som man ser av de overforstående grafene er det ikke slik at funksjonelle IKT-endringer alltid vurderes opp mot pasientsikkerhet eller forsvarlig helsehjelp. Der virksomhetene oppgir at de har vurdert forsvarlig helsehjelp er det oftest bare vurdert tilgjengelighet/bortfall, og bare unntaksvis er det gjort vurderinger av endring i funksjoner i kliniske program for helsepersonell. I under 50 % av analysene blir det vurdert om endringene fører til endret ressursbruk for helsepersonell.

### 3.1.5 Helsetilsynets refleksjoner og vurderinger av funn

**Klassifisering av kritiske systemer**
Når foretak vurderer kritikaliteten av IKT-systemer, må den viktigste parameteren være hvilken konsekvens bortfall av systemet har for pasientbehandling. Det er derfor underlig at virksomhetene i Helse Vest offisielt klassifiserer AMK-systemene som viktigere enn EPJ, radiologisystem og kurvesystem. De samme foretakene oppgir at bortfall av EPJ fører til uforsvarlig pasientbehandling innen en time, og at planlagte operasjoner utsettes allerede etter 15 minutter. Kritikalitet må vurderes opp mot konsekvens for pasientbehandlingen, men vi har merket oss at oversikten over kritiske system ikke gjenspeiler faktiske forhold. Kontaktpersoner oppgir at EPJ og elektronisk kurvesystem i praksis vil håndteres som kritiske system.

Samtlige foretak har forankret klassifiseringen av kritikalitet høyt oppe i foretaket. Dette tyder på at foretaksledelsen er bevisst prioriteringen av IKT-systemer.

**Systemer foretakene selv har driftsansvaret for**
En betydelig mengde systemer blir operativt driftet av foretakene selv.

Ett foretak oppgir å være ansvarlig for all infrastruktur for systemene de selv har det operative driftsansvaret for. Dette innebærer at det vil være to parallelle infrastrukturer, der brukerne må logge seg inn på spesifikke PC-er avhengig av hvilke system de skal benytte. Slike todelinger oppleves neppe som praktisk for brukerne, og kan skape utfordringer i klinisk arbeidsflyt, økte kostnader til utstyr og administrasjon. ›

«Helseforetaks-strukturen med én regional felles IKT-driftsleverandør samler fagmiljø, men øker også konsekvensen av hendelser ved at feil hos én leverandør kan påvirke mange sykehus over store geografiske områder samtidig.»

**Bortfall av alle IKT-baserte løsninger**

Det er få innsendte overordnede ROS-analyser for bortfall av IKT-baserte løsninger. Analysene som er sendt inn, mangler i tillegg analyse av konsekvensene av IKT-bortfall for pasientbehandlingen. Dette henger trolig sammen med at arbeid med risikoanalyser i stor grad gjøres av IKT-driftsleverandørene. Riksrevisjonen (3) peker også på at virksomhetene i spesialisthelsetjenesten mangler oversikt over mulige sårbarheter, bruker lang tid på å rette de, og har uklare ansvarsforhold og oppgavefordeling i forbedringsarbeidet. Slike forhold bidrar til å øke sannsynligheten for å bli rammet av alvorlige hendelser. Helseforetaksstrukturen med én regional felles IKT-driftsleverandør samler fagmiljø, men øker også konsekvensen av hendelser ved at feil hos én leverandør kan påvirke mange sykehus over store geografiske områder samtidig.

Ni virksomheter gir klinikkene ansvaret for å utarbeide beredskapsplaner og nødrutiner for IKT-bortfall som kan påvirke klinikkens evne til å yte helsehjelp. De overordnede risikovurderingene som er sendt inn er sannsynligvis av begrenset verdi i dette arbeidet, fordi de er utydelige på hva konsekvensene i praksis vil være. Er det innlysende for de som arbeider med nødrutinene i klinikkene at telefoni kan bli påvirket ved nettverksbrudd?

Virksomhetsovergripende nødrutiner bærer også preg av å være utarbeidet for kortvarige hendelser, med større fokus på å komme i gang med IKT-feilretting enn å opprettholde helsehjelp. Nødrutinene og beredskapsplanene må baseres på relevante og treffsikre risikoanalyser for å kunne bidra til å opprettholde forsvarligheten i pasientbehandlingen.

Det er sannsynlig at situasjoner med omfattende og langvarige IKT-bortfall inntreffer ved norske helseforetak. Flere hendelser har vært rapportert i media (13,14) og hendelsen i Østre Toten kommune viser at utbrudd av kryptovirus også kan skje i helsetjenesten (15,16). HelseCERT (17) og Riksrevisjonen (3) peker også på økende omfang av dataangrep mot helseinstitusjoner.

Kartleggingen viser at ingen av virksomhetene har analysert konsekvensene av langvarige IKT-bortfall tilstrekkelig. Helsedirektoratet har også påpekt manglende forståelse for hvor sårbare IKT-systemene er (18). Poenget med en risiko- og sårbarhetsanalyse (og/eller en beredskapsanalyse) er at man skal gjennomgå hendelsesforløp på en slik måte at tiltak kan identifiseres i forkant. En bør vurdere både sannsynlighetsreduserende og konsekvensreduserende tiltak. En beredskapsplan for å effektivt håndtere hendelsen (etter at den er oppstått) bør komme i tillegg til dette. ›

### Øvrige risikoanalyser

I to regioner har IKT-driftsleverandører ansvar for risikoanalyser knyttet til tilgjengelighet, integritet og konfidensialitet (informasjonssikkerhet), og helseforetakene har ansvar for risikoanalyser knyttet til forsvarlig helsehjelp. Helsetilsynet ser det som feil å skille mellom ansvar for informasjonssikkerhet og forsvarlig helsehjelp. Tilgang til riktige data til riktig tid er en forutsetning for å levere forsvarlige helsetjenester. Et eksempel på behov for riktige data gjelder legemiddelinformasjon der det i dag er en kjent høy risiko. Det er for mange uklart hvem som har ansvar for at helsepersonell skal bruke tid på å oppdatere legemiddelinformasjon i flere interne systemer. Det er også uklart hvem som har ansvar for arkitekturvalg som krever at helsepersonell må logge inn i flere ulike system for å sikre seg tilstrekkelig informasjon om pasienter. Denne manglende ansvarsavklaringen er en risiko i seg selv.

Den innsendte dokumentasjonen viser at det har oppstått uønskede hendelser i helsetjenesten på grunn av dårlig eller manglende funksjonalitet i IKT-systemer. Det er generelt for lite fokus på om løsningene er brukervennlige, og om det er elementer i systemene som kan skape risiko for pasientbehandlingen.

! Krav til konfidensialitet er håndfaste og krav til tilgjengelighet er målbare. Disse kravene brukes i utarbeidelse av tjenesteavtaler. Tilfredsstillende brukervennlighet, dataintegritet (samsvarende/oppdatert informasjon i ulike system), forsvarlige funksjoner og opplæring lar seg ikke like enkelt spesifisere, og vurdering av kliniske risikoer krever helsefaglig kompetanse. Den innsendte dokumentasjonen viser at risikoanalysene er svake på disse områdene.

Helsetilsynet ser det som uheldig at det brukes ulike definisjoner for informasjonssikkerhet i sektoren. Perspektivet med full dataintegritet i ulike systemer faller i mange sammenhenger bort. Samsvarende og oppdaterte pasientdata i ulike system kan være avgjørende i behandling av kritisk syke pasienter.

Formålet med bruk av IKT i helseforetak er å forbedre og effektivisere pasientbehandlingen. Manglende tilgjengelighet på informasjon om legemidler, allergier, behandlingsløp og annen kritisk informasjon kan medføre fare for at pasientskader oppstår. Risikoanalysene vektlegger i stor grad personvern og tilgjengelighet, og i liten grad evnen til å yte forsvarlig helsehjelp. Når man ser på kompetansen til de som lager tema og innhold i risikoanalyser, synes det å være varierende grad av deltakelse av helsepersonell. Dette kan være en av årsakene til at risikoanalysene har lite fokus på forsvarlig helsehjelp.

I de tilfeller hvor forsvarlig helsehjelp oppgis å være vurdert, er dette mange steder gjort ved at IKT-tilgjengelighet er vurdert. IKT-tilgjengelighet er viktig for å ivareta forsvarlig helsehjelp, men denne ›

grove kategoriseringen tar ikke høyde for innmeldte avvik knyttet til funksjonalitet eller brukervennlighet i EPJ, legemiddelsystem og øvrige fagsystem som helsepersonell er avhengig av for å kunne levere forsvarlig helsehjelp.

Samlet viser dette at IKT-risikovurderinger knyttet til pasientsikkerhet ikke er integrert i ledelse og kvalitetsarbeidet som forutsatt. Det ser ut som om det er et uheldig skille mellom teknisk sikkerhet (oppetid og personvern) og klinisk praksis (forsvarlig helsehjelp, pasientsikkerhet).

## 3.2 Kommunikasjon rundt ØH-innleggelser og transport av akutt syke

### 3.2.1 Bortfall av 113

13 av 17 helseforetak (75 %) som deltok i denne kartleggingen har egen AMK-sentral. Ett av disse foretakene har ikke øvd på bruk av nødrutinen for bortfall av medisinsk nødtelefon (113). De øvrige 12 helseforetakene med AMK-sentral svarer at de har øvd på nødrutinen i løpet av siste halvår.

Dersom AMK-sentralen mister tilgang til 113 og sentrale IKT-system, har 12 av virksomhetene avtale om overføring av AMK-funksjon til annen AMK i regionen. To av disse helseforetakene presiserer at de først vil forsøke å benytte lokale reserver. Et av foretakene har kun lokal reserveløsning. Ingen av foretakene har avtale om overtakelse med AMK-sentral i en annen region.

Helseforetakene ble også spurt om risiko for at den AMK-sentralen som skal overta ved ev. feil er rammet av det samme problemet. Svarene på spørsmålene varierte:

| | |
|---|---|
| Ja det er en liten risiko for at ulike AMK-sentraler rammes av samme feil (liten risiko, men høy konsekvens): | 6 |
| Risikoen er vurdert, vi har selvstendige AMK-sentraler som ikke er påvirket av hverandres installasjoner: | 5 |
| Dette er ikke vurdert: | 2 |

### 3.2.2 AMIS og Transmed

AMIS er et system som benyttes ved akuttmedisinske kommunikasjonssentraler (AMK), ved legevaktsentraler (LV) og i ambulansetjenesten i Norge. AMIS har full nasjonal utbredelse og benyttes ved alle AMK-sentraler i landet. AMIS har funksjonalitet for mottak og registrering av nødmeldinger (inkl. opprinnelsesmarkering), bestilling av ambulansetransport, henvendelser til legevakt ›

«To helseforetak nevner at Nødnett benyttes av sentrale og klinikkvise beredskapsstaber ved eventuelt bortfall av telefoni.»

(rådgivning eller ønske om lege hjem), gruppering, sortering og prioritering av oppdrag, koordinering og tildeling av ressurser (ambulanser og leger) til ventende oppdrag, tilbakemelding fra ressurs om status, tidspunkter, aksjonslogg, pasientoversikt ved større ulykker, ambulansejournal, søking på tidligere hendelser, oppdrag, pasienter og statistikk. Transmed brukes av alle ambulansesentraler for å holde oversikt over hvor ambulansene er og for å styre ambulansene.

Helseforetakene som har egen AMK-sentral ble spurt om øving i bruk av nødrutinen for AMIS. 10 av 13 helseforetak (77 %) hadde øvd personell i nødrutinen i perioden kartleggingen pågikk (juni til september 2020). Resterende helseforetak hadde øvd personell i bruk av nødrutinen siste halvår.

Helseforetakene som har egen AMK-sentral ble spurt om øving i bruk av nødrutine for Transmed. 8 av 13 helseforetak (62 %) hadde øvd personell i nødrutinen i perioden kartleggingen pågikk. Alle helseforetak hadde øvd personell i bruk av nødrutinen siste to år.

### 3.2.3 Nødnett

Alle benytter Nødnett i prehospitale tjenester som AMK, ambulanse og akuttmottak. Ved fem av virksomhetene benyttes Nødnett også ved intern varsling.

To helseforetak nevner at Nødnett benyttes av sentrale og klinikkvise beredskapsstaber ved eventuelt bortfall av telefoni. En virksomhet har oppgitt at Nødnett benyttes av vektertjeneste.

Virksomhetene ble spurt om hvert av disse bruksområdene for Nødnett også har en nødrutine for bortfall av Nødnett. 13 av 17 virksomheter (76 %) bekreftet dette. Fire virksomheter har svart 'annet' og lagt inn ulike kommentarer i svarene sine. Ett foretak mangler nødrutine i akuttmottak. Øvrige kommentarer viser til nødrutiner som er etablert via mobil- og satelittelefoner.

### 3.2.4 Helsetilsynets refleksjoner og vurderinger av funn

Alle AMK-sentralene har øvd på nødrutinene for de mest sentrale systemene sine. De har øvd på nødrutine for AMIS det siste halvåret, og de har øvd på nødrutine for Transmed i løpet av de siste to årene. De fleste øvelsene er gjort mens kartleggingen pågikk. Vi vet ikke om dette skyldes at de har rutine for å øve så ofte eller om denne kartleggingen utløste øvingene. ›

Etter hendelsene 22. juli 2011 utarbeidet Helsedirektoratet en evalueringsrapport (19). I denne er det flere anbefalinger som angår IKT-systemene som brukes:

- **Det må rutinemessig gjennomføres tekniske og operative sikkerhetsvurderinger av AMK-sentralene. Som en del av slike vurderinger må IKT-systemene belastningstestes.**
- **De regionale helseforetakene må sikre at det etableres systemer som gjør det mulig å holde oversikt over ambulanse- og luftambulanseressurser på tvers av AMK, foretaks- og regionale nivå. AMK-sentralene bør også kunne avlaste hverandre og utnytte hverandres kompetanse og kapasitet.**

I Oppdragsdokumentet fra regjeringen til de fire RHF-ene for året 2012 stod følgende mål: «Beredskapsplanene i regionen og i helseforetakene er oppdatert og tilpasset med utgangspunkt i erfaringene fra håndteringene av terrorangrepet 22. juli 2011 og andre tidligere hendelser.»

I flere av regionene benytter de ulike AMK-sentralene samme installasjon av AMIS og Transmed. Denne regionaliseringen har delvis skjedd etter 2011 og kan bety at ved overbelastning i et av de sentrale systemene, slik OUS opplevde under terrorangrepet, kan en overbelastning nå ramme alle AMK-ene i samme region.

På spørsmålet om hvordan innbyggerne sikres forsvarlig helsehjelp hvis AMK-sentralen mister tilgang til 113 og sentrale IKT-system, var det ingen som hadde avtale med AMK-sentral i annen region. Dette betyr at anbefalingen om samarbeid på tvers mellom AMK-ene ikke er på plass, selv om det har vært et mål for RHF-ene siden 2012. Kartleggingen viser at systemsvikt i noen regioner kan ramme alle AMK-er i regionen samtidig, og at det ikke finnes formelle avtaler om støtte fra AMK-er i andre regioner. Dette er alvorlig da det kan føre til at pasienter som ringer 113 ikke får svar, eller at ambulanser til akutt syke blir forsinket siden IKT-system for koordinering svikter.

Alle virksomhetene bruker Nødnett i AMK, ambulanse og akuttmottak. Utover det varierer bruken mye mellom de ulike virksomhetene. I et temadokument om Nødnett (20) skriver Helsedirektoratet:

«De regionale helseforetakene og kommunene skal sørge for at helsepersonell i vaktberedskap er umiddelbart tilgjengelig i Nødnett. Det gjelder helsepersonell ved AMK-sentraler og legevaktsentraler, helsepersonell i vaktberedskap i somatiske og psykiatriske sykehus med akuttfunksjon, og helsepersonell i ekstern vaktberedskap.»

Denne kartleggingen viser lite bruk av Nødnett for 'helsepersonell i vaktberedskap' utover prehospital tjeneste.

For Nødnett er nødrutinene basert på bruk av telefoni. Dette gjør det svært viktig at ikke alle telefonløsningene har felleskomponenter som gjør at de kan falle ut samtidig, noe som ikke er undersøkt i denne kartleggingen.

## 3.3 Diagnostisering av akutt syke ved IKT-bortfall

### 3.3.1 Estimert og opplevd oppetid for EPJ

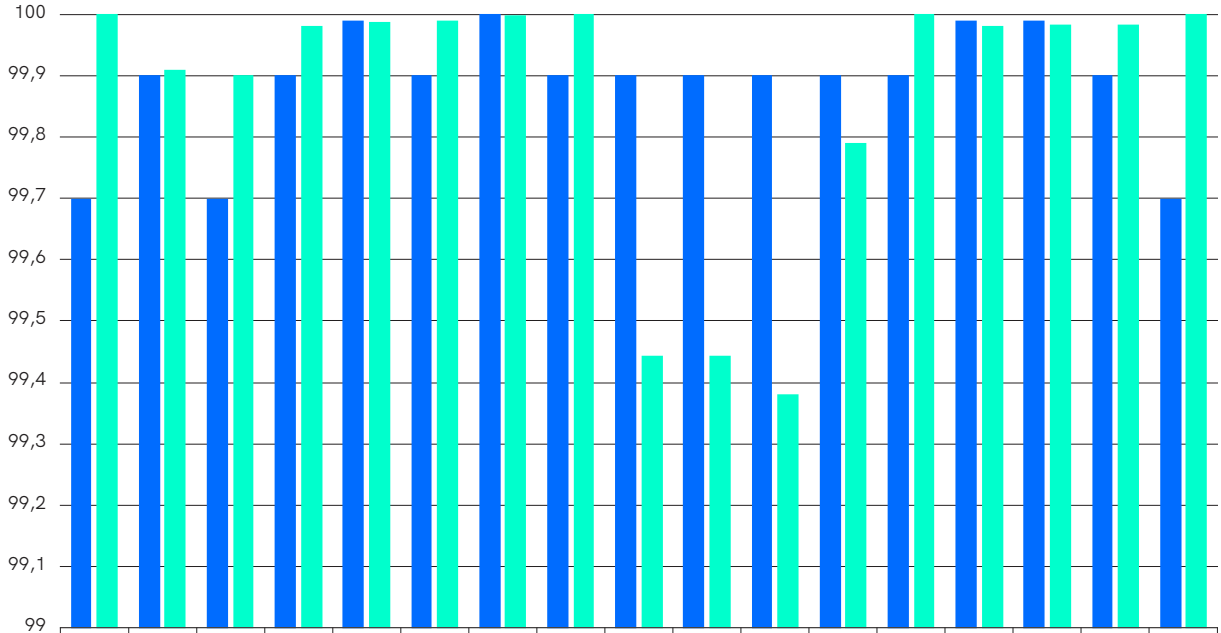
Alle IKT-driftsleverandører har avtalt 99,7 – 100 % oppetid for EPJ. Gjennomsnittlig har de estimert 99,88 % oppetid.

14 av 17 virksomheter (82 %) har svart at oppetid er estimert per måned og en har svart at oppetid er per år. I en måned med 31 dager vil 99,7 % oppetid bety 133 minutter utilgjengelighet. To av helseforetakene vet ikke hvilket tidsrom oppetiden er estimert for.

Virksomhetene ble også spurt om hvor mange minutter EPJ har vært utilgjengelig (uten lesekopi) ved akuttmottak i 2019. Fem virksomheter svarte at de ikke har slike målinger. Det var noe diskrepans i tall som ble meldt inn fra helseforetakene og IKT-leverandørene. Gjennomsnittet i de elleve foretakene som har oppgitt nedetid er ca. 587 minutter. Nedetiden fordelte seg forøvrig slik på de 12 virksomhetene som har slike målinger:

| Total nedetid | Virksomheter |
|---|---|
| Ingen | 2 |
| 10-50 minutter | 3 |
| 2-4 timer | 2 |
| 6 timer | 2 |
| 16,6 timer | 1 |
| 54 timer | 1 |
| 180 timer | 1 |

*Figur 3 Differanse mellom estimert (avtalt) oppetid og rapportert oppetid*




| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Estimert | 99,7 | 99,9 | 99,7 | 99,9 | 99,99 | 99,9 | 100 | 99,9 | 99,9 | 99,9 | 99,9 | 99,9 | 99,9 | 99,99 | 99,99 | 99,9 | 99,7 |
| Rapportert | 100 | 99,91 | 99,9 | 99,98 | 99,987 | 99,99 | 99,998 | 100 | 99,444 | 99,444 | 99,38 | 99,79 | 100 | 99,98 | 99,984 | 99,984 | 100 |

Virksomhetene ble også spurt om hvor mange minutter EPJ i tillegg har vært tilgjengelig i lesemodus, altså muligheten til å lese, men ikke tilføre eller endre journalinformasjon. 7 av 17 virksomheter (41 %) manglet målinger på dette. 6 av 17 virksomheter (35 %) hadde 0-20 minutters bruk av lesekopi og 4 virksomheter hadde 2-13 timer bruk av lesekopi i akuttmottak i 2019.

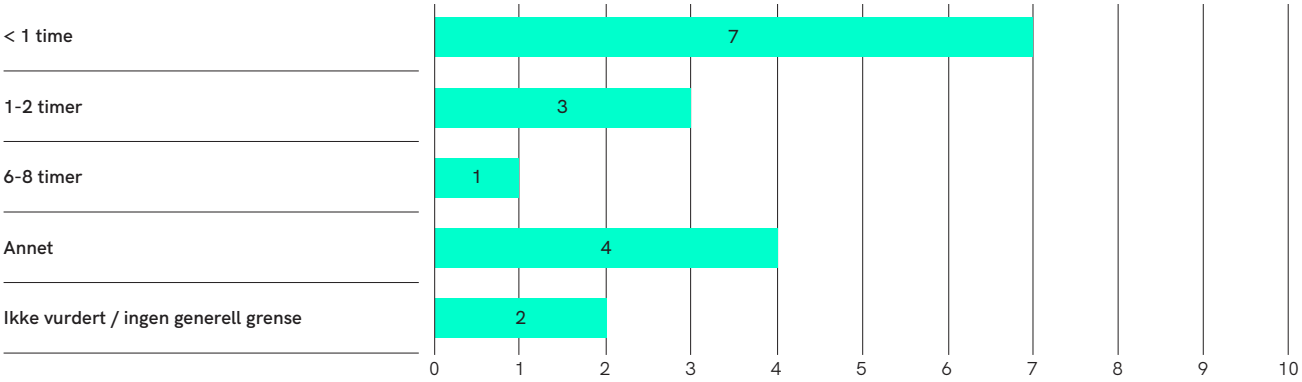
IKT-driftsleverandørene har rapportert om 100 % oppetid for EPJ ved fem virksomheter i 2019. For de øvrige 11 virksomhetene (65 %) med IKT-leverandør har leverandøren oppgitt at det er levert 99,38 - 99,99 % oppetid. Omtrent halvparten av virksomhetene har svart at dette er oppetid som er rapportert på sentral EPJ-database, og har kommentert at dette ikke er oppetid slik brukerne opplever den.

Pasientjournalsystemene kjører i parallelle datasentre, med redundans i alle deler av løsningene. Bortfall av et helt datasenter skal i teorien ikke føre til bortfall av systemene. Brukerne kan allikevel oppleve at systemet er utilgjengelig bl.a. på grunn av nettverksfeil. ›

### 3.3.2 Konsekvenser ved EPJ-bortfall

Virksomhetene ble bedt om å oppgi hvor lang tid det vil ta før det blir vesentlig risiko for svikt i noen forsvarlige helsetjenester når DIPS/DocuLive faller bort. Alle deltakerne har svart på dette spørsmålet.

*Figur 4 Tid før svikt i forsvarlige helsetjenester ved bortfall av DIPS/DocuLive*




Virksomhetene oppgir at bortfall av DIPS/DocuLive vil få konsekvenser for polikliniske konsultasjoner og oppstart av planlagt aktivitet som operasjoner, med mindre tilstrekkelig informasjon er tilgjengelig på grunn av gjennomført planlegging eller i andre systemer.

Fire virksomheter har lagt inn kommentar om at risikoen avhenger av situasjonen, slik som tid på døgnet og tilgang til andre medisinske fagsystemer. Eksempel på et typisk svar er:

«Dette er avhengig av ulike faktorer, f.eks tid på døgn, type avdeling osv. Bortfall mer enn 15 minutter medfører at operasjoner og polikliniske konsultasjoner må utsettes, mer enn 1 time bortfall medfører en vesentlig risiko for svikt i utførelsen av helsetjenester (pga. utsatte ØH operasjoner, risiko for feilmedisinering etc). EPJ–tilgang er forutsetningen for trygg pasientvurdering i mange akutte situasjoner og svikt i forsvarlighet inntrer få minutter etter en tilgang er borte.»

Én virksomhet har ingen generell tidsgrense og presiserer at nødvendig behandling oftest kan gjennomføres med reservesystem eller manuelle systemer. Én virksomhet svarer at de ikke har tatt stilling til utsendt spørsmål og ikke har vurdert risikoen for bortfall opp mot risiko for svikt i forsvarlig helsetjeneste.

Svar på dette spørsmål er gitt av medisinske fag- og linjeledere ved 14 av 17 virksomheter (82 %). For 3 av virksomhetene (18 %) er fagbakgrunn ukjent. ›

> «Ved langvarige IKT-bortfall vil de fleste sykehus etterhvert miste oversikt over inneliggende pasienter og ledig kapasitet.»

11 av 17 virksomheter (65 %) oppgir at ved bortfall av EPJ og radiologisystem vil noen operasjoner stanses midlertidig, men at alle operasjoner som er nødvendig for å gi forsvarlig helsehjelp utføres. 2 av 17 virksomheter (12 %) svarer at få eller ingen operasjoner påvirkes av IKT-bortfall, og 4 av 17 virksomheter (24 %) svarer «annet». Disse fire oppgir at det kan være flere kriterier som spiller inn enn svikt i EPJ og radiologisystem, og et typisk svar fra disse er:

«Hovedregel er at planlagt behandling utsettes/ikke starter opp, med mindre behandlende leger opplever de allerede har all nødvendig informasjon om pasienten (for eksempel fordi de har rukket å sette seg inn I pasienten ifbm precision/tilsyn dagen før). Nødvendig øyeblikkelig hjelp gjennomføres dersom reservesysten/manuelle systemer fungerer slik at man kan drive forsvarlig diagnostikk. Dersom disse systemene ikke fungerer vil kun akutt livreddere behandling gjennomføres, øvrige pasienter søkes overflyttet til andre kompetente sykehus.»

### 3.3.3 Oversikt over inneliggende pasienter ved bortfall av IKT

Virksomhetene ble spurt om de har nødrutiner for å opprettholde oversikt over inneliggende pasienter ved IKT-bortfall. Svarene på spørsmålet varierte noe.

2 av 17 virksomheter som deltok i kartleggingen, sendte inn nødrutiner for å holde en samlet oppdatert oversikt over inneliggende pasienter ved IKT-bortfall. En del sykehus svarer at sengepostene holder oppdatert oversikt over inneliggende pasienter hver for seg.

Sykehusene som klarer å vedlikeholde samlet oversikt over inneliggende pasienter ved IKT-bortfall bruker mottaket som koordinator. Alle avdelinger melder innleggelser, utskrivinger og overføringer av pasienter til akutt-mottak/mottaksklinikk, som manuelt oppdaterer en samlet pasientoversikt. Informasjon om nye innleggelser, overføringer og utskrivninger gjøres via telefon eller rørpost.

Mange sykehus kan ta ut nødrapporter som inneholder oversikter over inneliggende pasienter i det IKT-feilen opptrer, men rapportene blir ikke oppdatert. Ved langvarige IKT-bortfall vil de fleste sykehus etterhvert miste oversikt over inneliggende pasienter og ledig kapasitet.

På samme måte svarte kun to av virksomhetene at de klarer å opprettholde en oppdatert oversikt over planlagte pasienter ved bortfall av pasientadministrativt system. Disse oversiktene blir imidlertid ikke så raskt foreldet som oversikter over inneliggende pasienter. ›

Kommentar som kom fra et sykehus er:

«Det har ikke lykkes meg å finne spesifikke nødrutiner for denne oversikten. Det er likevel slik at mange avdeling har protokollført i GDPR-oversikten vår at de holder slike manuelle lister. Det kan virke som at hensynet mellom forsvarlig beredskap og personvern her tydeligere må diskuteres. Personvernhensyn tilsier at vi ikke skal ha fysiske lister utenom IT-systemene.»

### 3.3.4 Overordnet nødrutine for EPJ

Samtlige foretak oppgir at de både har overordnede nødrutiner for bruk ved bortfall av EPJ, og etablerte reserveløsninger for å gi tilgang til pasientdata ved en del typer IKT-feil.

Infrastrukturen rundt pasientjournalsystemene er oppgitt å være redundant for alle virksomheter, slik at DIPS/DocuLive vil være tilgjengelig, også ved bortfall av ett fysisk datasenter. Ved planlagte oppgraderinger og feilsituasjoner *med fungerende nettverk* kan brukerne styres mot en server som har en kopi av informasjonen i EPJ, men bare for lesing (lesekopi). Ved bruk av lesekopi har virksomhetene rutine for at ny pasientjournalinformasjon for det meste registreres på papir i oppholdsmapper, og etterregistreres når normaldrift gjenopprettes. Oppholdsmappene følger pasienten ved opphold på flere avdelinger. Virksomhetene har oppgitt at lesekopiløsningene har begrensinger sammenliknet med produksjonsløsningen. Eksempler er færre samtidige brukere, manglende innloggingsmulighet til Kjernejournal, manglende rekvirering, henvisninger, rapportering, meldingsutveksling med kommunene og prøvesvar.

Ved uforutsette hendelser oppgir foretakene at klargjøring av lesekopi av EPJ kan ta mellom 15 og 90 minutter, fra beslutning om etablering er tatt. Virksomhetene oppgir å ha beslutningsmyndighet ovenfor IKT-driftsleverandør om å etablere lesekopi. Beslutning gjøres av foretaksledelse eller krise-/beredskapsledelse avhengig om hendelsen er planlagt eller ikke. Virksomhetene har i stor grad satt opp kriterier for etablering av lesekopier. Eksempler på kriterier er lang eller ukjent forventet løsningstid ved feilsituasjoner, eller lang forventet nedetid ved planlagte hendelser.

Flere virksomheter har i tillegg egne PC-er der det kontinuerlig legges inn en kopi av relevante journaldata til inneliggende pasienter. Journalene kan skrives ut og distribueres i krisesituasjoner med fullstendig bortfall av EPJ. Denne løsningen er ikke avhengig av nettverk for å fungere, men det oppgis at det er et begrenset antall slike PC-er. Noen virksomheter oppgir også å ha en nettbasert løsning for dokumentasjon som erstatter papirjournaler. Omtrent halvparten av ›

virksomhetene oppgir å kunne skrive ut pasientrapporter med seneste journalnotat før planlagt nedetid. Avdelingene vurderer selv behovet for utskrifter ut fra situasjon og forventet nedetid.

2 av 17 virksomheter (12 %) har PC-er med mobilt bredbånd, og opprettholder dermed tilgangen til EPJ, også med informasjon om nye pasienter ved nettverksbortfall. Dersom nettverksbortfallet berører IKT-driftsleverandørens serverinfrastruktur, vil ikke denne typen løsning hjelpe.

! 5 av 17 virksomheter (29 %) har lokale lesekopier av EPJ som kan benyttes ved bortfall av eksterne nett, men som forutsetter at internt nettverk fungerer. Disse vurderes nå fjernet ved 3 virksomheter i Helse Nord, og det pågår arbeid med å avklare nye reserveløsninger.

1 av 17 virksomheter (6 %) har mulighet til å etablere tilgang til lokal EPJ-database ved akuttmottak ved langvarige nettverksbortfall. De kan trekke fysisk kabel til en EPJ produksjons- eller lesekopi database.

**Øvelser**
13 av 17 virksomheter (76 %) oppgir å ha øvd på nødrutinene for EPJ i 2020. To oppgir å ha øvd i løpet av 2019, to foretak oppgir å aldri ha øvd på nødrutinen.

### 3.3.5 Tilgang til kritisk informasjon når IKT feiler

Manglende tilgang til Kjernejournal ved bortfall av DIPS/DocuLive var ukjent for flertallet av virksomhetene i kartleggingen, og svarene var initialt noe uklare. Gjennom oppfølgingssamtaler ble det avklart at det ikke er mulig å bruke Kjernejournal som en nødløsning ved bortfall av EPJ i andre regioner enn Helse Vest. I Helse Vest kan de logge på Kjernejournal også via kurvesystemet Meona og AMK-systemet AMIS.

### 3.3.6 Bestilling/svar på blodprøver og radiologiske undersøkelser når IKT-løsningene ikke fungerer

Virksomhetene ble spurt om de har nødrutiner for sikker og effektiv bestilling/svar på blodprøver og radiologi når IKT-løsningene ikke fungerer. 15 av 17 av virksomhetene (88 %) svarte at de har slike rutiner. Dette inkluderer de som svarte at de kun bruker papirrekvisisjoner som nødrutiner. 2 av 17 virksomheter (12 %) svarte at de delvis har slike nødrutiner. ›

«Det ble rapportert 3 tilfeller der EPJ var utilgjengelig ved 3 ulike akuttmottak i mer enn 15 timer. Ingen av de rammede akuttmottakene hadde nødrutiner for tilgang til journalopplysninger.»

De innsendte dokumentene er både versjoner av papirrekvisisjonene og dokumenter som beskriver nødrutinene som skal iverksettes dersom IKT-løsningene ikke fungerer. Noen av de innsendte nødrutinene gir oversikt over roller og ansvar ved bortfall av IKT-løsningene. Fokus for de innsendte nødrutinene er å sikre den akuttmedisinske driften. Andre problemstillinger som for eksempel polikliniske problemstillinger utsettes til systemet er tilbake i vanlig drift. Et typisk svar fra en virksomhet er: «Grunnet vanskelig arbeidsflyt for radiologiene vil kun de undersøkelsene der svar har akutt diagnostisk konsekvens få midlertidig svar» (Fra Vestre Viken, nødrutiner ved nedetid på PACS.)

### 3.3.7 Øvelser i bruk av nødrutiner for bortfall av radiologisystem/RIS/PACS system

Virksomhetene ble spurt om når helsepersonell sist øvde på bruk av nødrutinen for bortfall av radiologi-/multimediasystem. Ved fire virksomheter har personell øvd på bruk av nødrutinen de siste seks måneder. Ved åtte virksomheter har personell øvd på bruk av nødrutine for 6-20 måneder siden. Ved fem virksomheter har ikke personell øvd på bruk av nødrutinen for bortfall av radiologi-/multimediasystem.

### 3.3.8 Helsetilsynets refleksjoner og vurdering av funn

**Oppetid for EPJ og konsekvenser for pasientbehandling**
Utilgjengelige helseopplysninger er en fare for pasientsikkerheten. Risikoen for uønskede hendelser øker jo lengre IKT-bortfall varer, ved akutt sykdom eller dersom sykehistorien ikke er kjent for behandler. Det ble rapportert 3 tilfeller der EPJ var utilgjengelig ved 3 ulike akuttmottak i mer enn 15 timer. Ingen av de rammede akuttmottakene hadde (nødrutiner for) tilgang til EPJ.

Det er positivt at alle virksomheter har tjenesteavtaler for å sikre høy oppetid for EPJ. En utfordring er at noen virksomheter kan ha godtatt avtaler som er for lite spesifikke på hvilket tidsrom oppetiden er avtalt for, og kan dermed ha akseptert lengre nedetid enn antatt. Virksomhetene har også få eller ingen sanksjonsmuligheter mot IKT-leverandørene ved brudd på avtalene. Det er viktig at virksomhetene har høy bevissthet om hvilke avtaler om oppetid de har inngått med sine driftsleverandører, og om hvilke nødrutiner som er tilgjengelige for de ansatte.

Virksomhetene vurderer tilgang til informasjonen i DIPS/DocuLive til å være så kritisk at bortfall raskt fører til risiko for svikt i muligheten til å yte forsvarlig helsehjelp. Det gis fortsatt nødvendig øyeblikkelig hjelp, men med økt risiko på grunn av manglende tilgang til informasjon om ›

pasientene. Bortfall av EPJ kan ha betydning for liv og helse, og vil i mange situasjoner føre til forsinket behandling. Lengde på og omfang av IKT-svikten har likevel stor betydning, og deler av pasientbehandlingen vil kunne fortsette dersom andre fagsystemer fortsatt er tilgjengelige. Det er likevel ikke forsvarlig at EPJ er utilgjengelig i akuttmottak, og alle virksomheter må etablere nødløsninger for å sikre journalinformasjon om nye pasienter.

! Videre kan nødløsninger (eksempel pc med mobilt bredbånd) hos nøkkelpersonell, som koordinatorer i akuttmottak og sentraloperasjon, bidra til å opprettholde behandlingstilbud og forsvarlighet ved en del IKT-feil.

! Det er ikke bedt om eller sendt inn rutiner for å varsle instanser utenfor virksomhetene ved IKT-bortfall. Helsetilsynet har mottatt varslingssak der informasjon fra ekstern henvisning ikke var tilgjengelig ved planlagt nedetid i DIPS. Virksomhetene må varsle om planlagt og pågående ikke-planlagt nedetid eksternt. Eventuelt må samarbeid sikres ved at alle pasienter innlagt som øyeblikkelig hjelp får en papirhenvisning med seg ved innleggelse på sykehus.

Vurderingen av risiko ved IKT-bortfall er forankret på høyt nivå i virksomhetene, og samtlige virksomheter har innført omfattende tekniske tiltak for å minimere sannsynligheten for bortfall.

I videre arbeid er det nødvendig at virksomhetene ser nærmere på beslutninger og risikovurderinger vedrørende tidspunkt og lengde på planlagt nedetid for EPJ, samt informasjon til samhandlende legevakter for overføring av henvisninger i planlagt nedetid.

### Overordnet nødrutine for EPJ

En del virksomheter har løsninger for å få tilgang til journaler for inneliggende pasienter dersom IKT feiler, men ingen virksomheter har per i dag tilgang til journaldata for nye pasienter dersom sentrale servere og nettverk feiler. Dette kan være en betydelig risiko for pasienter som kommer til akuttmottak. Nødrutinene baseres i stor grad på papirdokumentasjon og at informasjonsutveksling som normalt understøttes av EPJ gjøres telefonisk.

Ved omfattende bortfall vil nødrapporter gi tilgang til pasientinformasjon for inneliggende pasienter ved noen virksomheter. Nødrapportene vil kunne bidra til at virksomhetene kan opprettholde deler av behandlingstilbudet, men vil likevel ha begrenset nytteverdi. Dette fordi nødrapportene ikke inneholder journalinformasjon om pasienter som blir innlagt etter at IKT-feil har oppstått. Man risikerer som nevnt at akuttmottak må behandle pasienter uten informasjon om ›

> «Det er risikofylt at virksomhetene kun planlegger for kortvarige bortfall, og ikke har planlagt for tiltak ved langvarige og omfattende IKT-hendelser.»

relevant sykehistorie eller videresende pasienter til et annet sykehus i regionen.

Frittstående PC-er med mobilnett, med mulighet for innlogging til EPJ og Kjernejournal, kan gi tilgang til journalopplysninger ved bortfall av nettverk. De kan allikevel være sårbare for hendelser som eksempelvis virusutbruddet i Østre Toten (15,16) eller «Hydro-saken» (21), fordi de fortsatt er avhengige av at både mobilnett og sentrale servere er tilgjengelige. Funnene i kartleggingen viser at ingen sykehus ville hatt tilgang til EPJ-opplysninger ved slike hendelser.

Det er risikofylt at virksomhetene kun planlegger for kortvarige bortfall, og ikke har planlagt for tiltak ved langvarige og omfattende IKT-hendelser. I de fleste virksomheter vil elektiv behandling i stor grad stanses, noe som kan oppleves som frustrerende for pasientene som må sendes hjem og som engster seg for redusert prognosetap.

### Oversikt over inneliggende pasienter ved bortfall av IKT

Alle sykehus må sikre at de har kontinuerlig oppdatert oversikt over inneliggende pasienter ved IKT-bortfall. To sykehus klarer som nevnt dette, og praksis fra disse sykehusene bør være læring for resten av landets sykehus.

Helsetilsynet oppfatter det som en misforståelse ved enkelte virksomheter at GDPR står i veien for å kunne etablere forsvarlige nød- og beredskapsrutiner. Virksomhetene er ansvarlige for å gjøre forholdsmessige vurderinger av pasientsikkerheten opp mot personvernhensyn. Risikovurderingene av personvern og pasientsikkerhet må vektes mot hverandre, og det må planlegges for best mulig løsning for å ivareta begge hensyn.

### Tilgang til Kjernejournal når DIPS/DocuLive ikke fungerer

Det ble i løpet av kartleggingen avklart at det ikke er mulig å bruke Kjernejournal som en nødløsning ved bortfall av EPJ i andre regioner enn Helse Vest. I Helse Vest kan en logge inn i Kjernejournal via kurvesystem eller AMIS. Denne muligheten benyttes ikke så ofte (bare 6 % av virksomhetene i kartleggingen svarer at pålogging til Kjernejournal ved bortfall av EPJ noen ganger blir gjort).

Det kan være ulike grunner til at Kjernejournal ikke benyttes som en nødløsning ved bortfall av EPJ. Helsepersonell kan for eksempel ha opplevelser av at Kjernejournal inneholder lite pasientinformasjon, eller helsepersonell er kanskje ikke klar over at de har tilgang til Kjernejournal via andre system når EPJ er utilgjengelig. ›

### Nødrutine for bestilling/svar på blodprøver og radiologiske undersøkelser

Det er ikke mulig å trekke klare konklusjoner om hvorvidt nødrutinene sørger for sikker og effektiv bestilling/svar på blodprøver og radiologiske undersøkelser når IKT-løsningene ikke fungerer.

Det er imidlertid mulig å gjøre noen refleksjoner på bakgrunn av de innsendte dokumentene. Ved utarbeidelse av nødrutiner er det viktig å arbeide med realistiske scenarioer: Hvilket/hvilke system er nede? Er nettverket nede? Hvilke konsekvenser får driftsstansen på arbeidsflyten? Et papirskjema utgjør ikke en nødrutine. Papirskjema er en måte å understøtte arbeidsflyten når ett eller flere systemer er nede, men spesielt i store sykehus kreves det at roller og ansvar i nødrutiner er avklart.

Vi oppfatter nødrutiner som inneholder følgende elementer som nyttige og gjengir her for læring:

- *Hvordan man endrer arbeidsflyt ved de berørte avdelingene:* Nedetid fører til ressursknapphet i virksomheten. Hvilke undersøkelser blir ikke utført dersom det er driftsstans? Det er like viktig å vite hva man ikke skal bruke tid på som hva man skal bruke tid på. Dette sikrer en felles forståelse av hva som er mulig å gjøre i en driftsstanssituasjon. Slik tar man på alvor hvilken konsekvenser nedetid vil få for driften.
- *Hvem prioriterer hvilke oppgaver som skal utføres ved de berørte avdelingene:* Denne rollen kan ligne på den som har ansvar for triage ved en masseskadehendelse, bortsett fra at her gjelder masseskadehendelsen bortfall av samhandlingsverktøy og informasjon.
- *Forskjeller i arbeidsflyt:* Ved planlagt driftsstans vil man endre arbeidsflyten på en annen måte enn ved en uforutsett driftsstans, fordi man ved en planlagt driftsstans har tid til å igangsette ulike kompenserende tiltak før nedetiden trer i kraft. Ved en uforutsett driftsstans påvirker nedetiden driften umiddelbart.
- *Arbeidsflyten etter at systemene er i vanlig drift:* Nedetid fører til akkumulasjon av informasjon, enten registrert på papir, eller registrert i alternative elektroniske løsninger. En nødrutine må inneholde en plan for hvordan man får denne informasjonen tilbake i de rette systemene innen rimelig tid etter driftsstans.

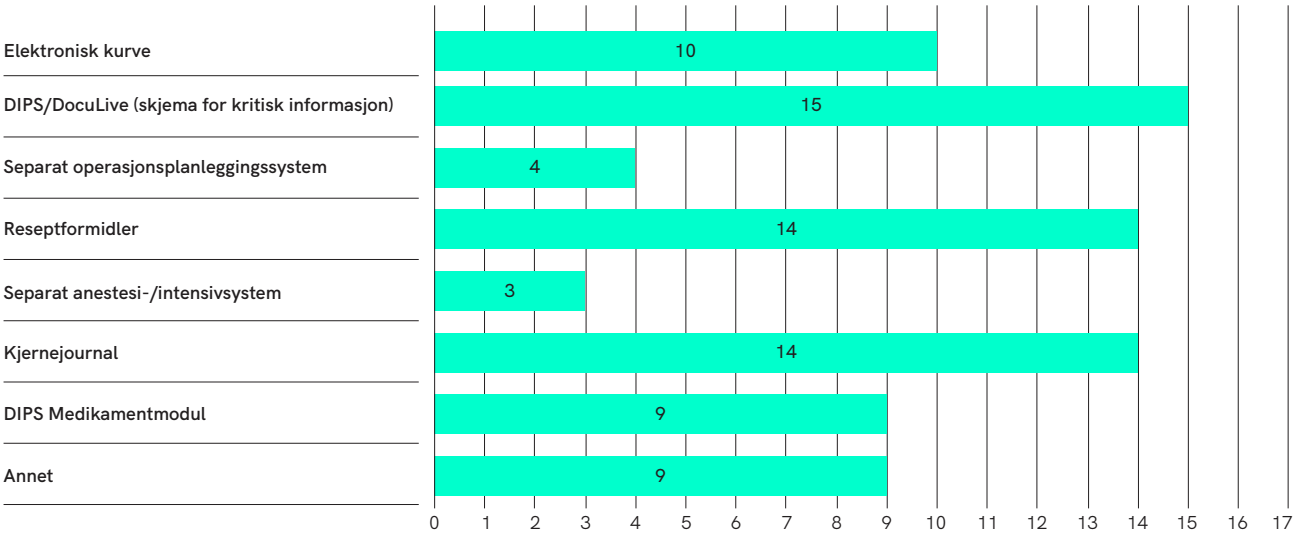
Det er urovekkende at 5 virksomheter ikke har øvd på bruk av nødrutinen for bortfall av radiologisystem. ›

## 3.4 Forsvarlig tildeling av legemiddel ved bortfall av IKT

### 3.4.1 Legemiddelinformasjon, dataintegritet og tilgang til oppdatert informasjon ved IKT-bortfall

Alle virksomheter ble bedt om å oppgi hvilke kliniske systemer de har legemiddelinformasjon om pasienter i. Svarene viser grad av tilgjengelighet og behov for integritet i legemiddelinformasjon (oppdaterte og riktige data i alle system).

*Figur 5 I hvilke IKT-system finnes informasjon om legemiddelbehandling som pasienten mottar, og eventuelle legemiddelallergier?*




I rubrikken annet ble følgende systemer nevnt: radiologi/RIS/PACS-systemer, fødesystem, anestesikurve, system for medikamentell kreftbehandling.

Fordelingen over antall foretak med mange IKT-system med legemiddelinformasjon fordeler seg slik:

| Virksomheter | Antall system |
|---|---|
| 7 | 6-7 |
| 9 | 4-5 |
| 1 | 3 |

> «Virksomhetene ble også spurt om informasjon om legemiddelbehandling/-allergi automatisk blir synkronisert mellom systemene. De fleste svarte at informasjonselementer ikke blir automatisk overført, men må manuelt skrives inn i de ulike systemene.»

Foretakene med færrest antall IKT-systemer med legemiddelinformasjon, har ikke innført elektronisk kurve enda.

Virksomhetene ble også spurt om informasjon om legemiddelbehandling/-allergi automatisk blir synkronisert mellom systemene. De fleste svarte at informasjonselementer ikke blir automatisk overført, men må manuelt skrives inn i de ulike systemene. To overføringer er unntaksvis laget. I Helse Sør-Øst overføres noen reaksjoner på legemidler automatisk mellom DIPS og elektronisk kurve MetaVision, men dette er avhengig av hvilke felt som benyttes i DIPS. I Helse Midt-Norge henter forskrivningsmodulen legemiddelreaksjoner fra DocuLive dersom de er angitt med ATC-kode.

Virksomhetene ble også spurt om antall separate IKT-systemer helsepersonell må logge seg inn i for å få en komplett oversikt over legemiddelinformasjonen. Noen systemer har funksjoner som åpner andre fagsystemer slik at de ikke krever en egen innlogging. Antall pålogginger er dermed noe lavere enn antall separate systemer. Kjernejournal, kurve, reseptmoduler og kritiske informasjon i EPJ er ofte tilgjengelig via en enkelt pålogging. Det mangler svar vedrørende nøyaktig antall pålogginger fra mange virksomheter. Helsepersonell må i noen sammenhenger logge på to til fire separate systemer for å få tilgang til legemiddelinformasjon.

### 3.4.2 Elektronisk medikamentkurve

Elektronisk medikamentkurve er helt eller delvis innført ved 13 av 17 helseforetak som deltok i kartleggingen.

4 av 13 virksomheter (31 % av virksomhetene med elektronisk kurve) har nødrutine som sikrer sikker utdeling av legemiddel når elektronisk kurveløsning ikke fungerer.

9 av 13 virksomheter (69 % av virksomhetene med elektronisk kurve) svarer at nødrutinen delvis sikrer sikker utdeling av legemiddel når elektronisk kurveløsning feiler. Et foretak forklarer risikoen slik:

«Avhengig av om det er planlagt eller ukontrollert. Ved ukontrollert nedetid vil mange brukere måtte vente på utskrift av legemiddellister og listene kan mangle dokumentasjon pga. frekvens for generering av nødrapporter. Frekvens på nødrapporter for MetaVision er satt opp etter anbefalinger fra HSØ. Disse er 12 timer frekvens for sengepost og annen hver time for intensiv, operasjon, akuttmottak. Nye innleggelser i mellom disse tidene er avhengig av at personell kan historikken.» ›

### 3.4.3 Helsetilsynets refleksjoner og vurdering av funn

7 sykehus har legemiddelinformasjon i 6 til 7 ulike IKT-system. Det kan dermed være vanskelig for helsepersonell å få oversikt over pasientens legemiddelbruk og ev. legemiddelallergier. Flere systemer fører til unødvendig tidsbruk for helsepersonell, både fordi man må bruke tid på innlogging for å få tilgang til opplysningene i mange systemer. Ofte må pasienten søkes opp på nytt og helsepersonell må også dokumentere/oppdatere samme opplysningen flere steder. Leger kan dermed miste oversikt over gjeldende legemiddelbruk, gjøre feil vurderinger, og sykepleiere kan dele ut legemiddel på sviktende informasjonsunderlag.

I lov om behandlingsrettede helseregistre (pasientjournalloven § 7) står det at løsninger skal «...understøtte pasientforløp i klinisk praksis og være lett å bruke og å finne frem i». De nevnte utfordringene var godt kjent allerede i utredning av Meld. St. 9 Én innbygger – én journal 2012-2013: «Også internt i større helsevirksomheter finnes det «siloer». Klinikere sine vansker med å få oversikt i ulike kliniske system er en av de største utfordringene i dagens systemporteføljе (22).

Opplysninger om pasienter og brukere kan ligge i ulike fagsystemer som diabetes-, fødsels- eller radiologisystemer, i det «primære» journalsystemet for dokumentasjon, i elektronisk kurvesystem og i systemer knyttet til medisinsk teknisk utstyr. Til tross for at utfordringene var kjent allerede i 2012, er det i de fleste virksomheter i ettertid innført nye system med duplikate data og nevnte krav til ekstra pålogging, ekstra søk på pasient og ekstra oppslag for helsepersonell. Eksempel på slike system er elektroniske kurvesystem og system for medikamentell kreftbehandling. Det skal i tillegg innføres Pasientens legemiddelliste som et felles system for primær- og spesialisthelsetjenesten. For å sikre pasientsikkerhet og brukervennlighet er det viktig at pasients legemiddelliste integreres med eksisterende elektroniske medikamentkurver.

Siden helseregionene velger flere separate løsninger (for eksempel for medikamentell kreftbehandling) blir det unødvendig ekstra forvaltningsarbeid fordi gjenbruk av kompliserte protokoller i legemiddelbehandlingen er vanskelig.

Under innføring av elektronisk kurve er det en tilleggsrisiko at en har ulike papir- og kurvesystem på ulike avdelinger. Alle manuelle overføringer av legemiddelopplysninger er potensielle feilkilder som vi vet jevnlig fører til avvik. Det er en risiko når en veksler mellom papir og ulike elektroniske kurver, eller når en veksler mellom ulike legemiddelsystem i et pasientforløp. Endring til felles system bør i prinsippet planlegges godt og gjøres over korte tidsperioder for å redusere tidsperioder med manuelle overføringer mellom ulike system. ›

Innføring av elektroniske medikamentkurver er en sentral del av digitaliseringen av klinisk dokumentasjon. Kurvene er et av de mest sentrale hjelpemiddel i klinisk virksomhet. Legemiddelfeil er en kjent og betydelig pasientrisiko. Elektroniske medikamentkurver er under innføring på alle kliniske avdelinger i spesialisthelsetjenesten. Det er betenkelig at en stor del av helseforetakene som har elektronisk medikamentkurve svarer at nødrutinen for medikamentutdeling bare delvis sikrer forsvarlig legemiddelutdeling.

## 3.5 E-konsultasjoner

### 3.5.1 Vurderes helsefaglige tema i risikoanalyser av e-konsultasjoner?

Det er sendt inn risikoanalyser vedrørende e-konsultasjoner fra 12 av 17 forespurte helseforetak (71 %). Noen helseforetak har sendt inn samme vurdering fra sine regionale IKT-leverandører.

Virksomhetene ble bedt om å oppgi hvilke helsefaglige tema som ev. var vurdert. De svarte noe varierende på dette:

*Tabell 2 Helsefaglige tema som er vurdert i risikoanalyser av e-konsultasjoner*

| | Svar | |
|---|---|---|
| Ikke gjort risikovurdering med fokus på forsvarlig helsehjelp | 5,88 % | 1 |
| Utilstrekkelig undersøkelse/anamnese og forsinket helsehjelp | 17,65 % | 3 |
| Utilstrekkelig undersøkelse/anamnese og feil behandling | 11,76 % | 2 |
| Uoversiktlig og feil legemiddelbehandling | 00,00 % | 0 |
| Fordeler med tanke på smitterreduksjon, ønske fra pasient i psykiatri og andre fordeler | 35,29 % | 6 |
| Annet (vennligst spesifiser) | 76,47 % | 13 |
| **Totalt antall respondenter** | | 17 |

Under 'Annet' har de fleste svart at de støtter seg på regionale vurderinger med hovedfokus på konfidensialitet og tekniske løsninger. Et par foretak svarer at vurdering av forsvarlighet gjøres etter klinisk skjønn for den enkelte pasient.

Få klinikere har deltatt i utarbeiding av risikoanalysene som er sendt inn.

Gjennomgang av de tilsendte risikoanalysene viser at hovedfokus er på konfidensialitet. Dette er vurdert i alle innsendte risikoanalyser. Tilgjengelighet, forsvarlig helsetjeneste, brukervennlighet og/eller ›

identifisering av riktig pasient blir vurdert i 2 til 7 av de innsendte dokumenter.

Vedlagt denne rapporten ligger et eksempel på prosedyre som innebærer vurdering av faglig forsvarlighet for pasienter som kalles inn til videokonsultasjon ved Oslo Universitetssykehus (Vedlegg 2). Eksempel på forhold som skal vurderes for alle pasienter, er pasientens teknologikompetanse, språklige barrierer og syn-/hørselshemming. Lignende vurdering er tilsendt fra Sørlandet sykehus: «Pasient som deltar i videokonsultasjon bør være utredet og diagnostisert og kjent av behandler eller samarbeidende helsepersonell».

9 virksomheter svarer at ingen avvik vedrørende e-konsultasjon er registrert. 6 helseforetak har registrert avvik knyttet til e-konsultasjoner siste halvår. Gjennomsnittlig antall avviksaker for disse 6 HF er 8 avvikssaker.

Tema for avvikene sorterte seg slik:

- 14 rot i innkallingene
- 16 tekniske feil (overvekt hos de som bruker NHNs videoløsning)
- 6 brudd på konfidensialitet
- 6 med ikke optimal behandling, 1 alvorlig
- 4 diverse

13 % av de rapporterte avvikene omhandlet kvaliteten på helsetjenesten som ble ytt under e-konsultasjonene.

### 3.5.2 Helsetilsynets refleksjoner og vurdering av funn

Virksomhetene har sendt inn svært få risikoanalyser av e-konsultasjoner som en metode for å gi forsvarlig helsehjelp. Dette kan henge sammen med at løsningene initialt ikke er vurdert som kritiske for å behandle pasienter, og at e-konsultasjoner først viste seg som veldig nødvendig metode etter at pandemien inntraff. Prioritering av fokus henger nok også sammen med overnevnte ansvarsfordeling (kap. 3.1.4) for risikoanalyser. Mange helseforetak oppgir at de har IKT-driftsleverandør som gjør risikoanalyser knyttet til informasjonssikkerhet og ressursbruk knyttet til IKT-personell. Samtidig oppgir IKT-driftsleverandørene at helseforetakene skal gjøre øvrige risikoanalyser knyttet til forsvarlig helsehjelp. ›

Risikoanalyser av e-konsultasjoner som en metode for å gi forsvarlig helsehjelp, er bare gjort ved et par helseforetak. Alle har vurdert personvernaspektet ved metoden. For å redusere smitte under pandemien er det fornuftig for helseforetak å vekte risiko for smitte større enn annen risiko for svikt i helsetjenesten når en ny og ukjent pandemi inntreffer.

Etter hvert bør en utarbeide løsninger, risikoanalyser og kliniske retningslinjer for bruk av e-konsultasjoner som tar med ulike aspekter vedrørende forsvarlig helsehjelp og informasjonssikkerhet. Risikovurderingene må vektes mot hverandre, og virksomhetene må planlegge for best mulig løsning for å ivareta begge hensyn.

Hensyn til pasientenes helsetilstand er viktigst. Videre må vurdering av pasientens preferanser for eksempel knyttet til reisevei og evne til å kommunisere via digitale flater, tas med i individuelle risikovurderinger for ulike pasientgrupper. Digital helsehjelp kan ha positiv effekt på både kvalitet, effektivitet og tilfredshet i helsetjenesten. Effekten vises blant annet gjennom redusert bruk av fysiske helsetjenester, og ved at digitale tjenester kan bidra til økt oppmøte til konsultasjon og bedre etterlevelse av helsepersonellets anbefalinger. Noen pasientgrupper kan også oppleve bedret tilgjengelighet til hjelp ved bruk av videokonsultasjoner (23, 24). På den andre siden vil sårbare grupper som i dag har lav digital kompetanse kunne øke fremtidige samfunnskostnader knyttet til helsetap, helsetjenestekostnader og produksjonstap (25).

Det bør også være mulig å luke bort tekniske feil og rot i innkallinger/koordinering av e-konsultasjoner som beskrevet i mange avvik i 2020.

## 3.6 Intern kommunikasjon/koordinering i sykehuset ved IKT-bortfall

### 3.6.1 Beredskapsorganisasjon

Alle virksomhetene har oppgitt å ha en beredskapsledelse som de benytter i ulike typer beredskapssituasjoner. 10 virksomheter har sendt inn overordnede beredskapsplaner, og 7 av disse beskriver tiltak ved IKT-hendelser. Handlingene ved IKT-hendelser er i stor grad rutiner for når og hvordan virksomheten raskt skal kunne starte arbeid med feilretting og innkalling av ekstraressurser, og at klinikkene skal ta i bruk egne planer og nødrutiner.

Beredskapsplanene som er sendt inn, beskriver rutiner for når foretakene etablerer krise- og beredskapsstab. Det oppgis kriterier for hendelser som umiddelbart kan føre til at foretaket kaller inn krisestab og går over i beredskapsdrift. Eksempler på dette er om EPJ er helt utilgjengelig, eller om uforutsette driftsstanser varer lengre enn to ›

«Foretak forutsetter tilgjengelige telefonitjenester for å kunne tilby forsvarlig helsehjelp ved omfattende IKT-bortfall.»

timer. I noen foretak er det oppgitt at AMK har en koordinerende funksjon, og kan være kontaktpunkt for melding av feil. AMK oppgis da å bidra i arbeidet med å fastsette beredskapsnivå, mobilisere beredskapsorganisasjonen, og varsle både internt og eksternt. I andre foretak oppgis det at denne funksjonen kan ivaretas av vakthavende lege, IKT-vakt, beredskapsvakt, IKT-driftsleverandør eller en kombinasjon av disse. Virksomhetene oppgir at de også har myndighet til å bestille beredskapsnivå hos sin IKT-leverandør, som forplikter seg til å bistå helseforetaket til situasjonen er avklart.

Varsling om endring av beredskapssituasjon oppgis å kunne skje via telefon, epost, HelseCIM, høyttaleranlegg, meldingstjenester, intranett, eller ved overbringelse og andre tilgjengelige kanaler. Videre oppdateringer kan gjøres via de samme kanalene, samt i egne informasjonsmøter. Ledere på alle nivåer oppgis å være ansvarlige for å formidle tilgjengelig informasjon ut til egne enheter. Enhetene rapporterer status og utvikling tilbake via tjenestevei. Eksempel på rapportinnhold er informasjon vedrørende tilgang til og behov for personell, lokaler, utstyr, medikamenter, konsekvenser for ordinær drift og behov for støtte. Det er eksempler på at sluttbrukere har ansvaret for å direkte varsle beredskapsvakter når det oppdages feil, samt å ta i bruk nødrutiner som manuell varsling av stansteam eller andre. Telefonnummer til alarmtelefoner til personell med slike vakt- eller beredskapsroller oppgis å være tilgjengelige på fysiske plakater som er plassert ut på klinikkene.

### 3.6.2 Telefoni (mobil-, analog-, IP-telefon eller DECT)

Bortfall av telefoni og personsøker-/callingsystemer er oppgitt å være spesielt kritiske, fordi vakthavende helsepersonell (som traume-, hjertestans- og trombolyseteam) tilkalles over telefonisystemer. Tilkalling av personell med hjemmevakt eller beredskapsfunksjoner gjøres også telefonisk, og enkelte foretak har derfor krav til at lister med private telefonnumre er utarbeidet og tilgjengelig på avdeling. Foretak forutsetter tilgjengelige telefonitjenester for å kunne tilby forsvarlig helsehjelp ved omfattende IKT-bortfall. Eksempelvis kan rekvirering og innhenting av prøvesvar gjøres muntlig over telefon. Innsendte nødrutiner viser også begrenset operasjonskapasitet dersom telefonisystemer er utilgjengelige.

Mange helseforetak oppgir å benytte datanettet til telefoni. Bortfall av datanettet får da som konsekvens at både telefonitjenester og tilgang til applikasjoner kan slutte å fungere samtidig. ›

De innsendte beredskapsplanene og nødrutinene nevner flere mulige kommunikasjonskanaler ved bortfall av telefonisystemer:

- Bruk av privateide mobiltelefoner og telefonlister til viktige funksjoner og beredskapsvakter
- Direktemeldingssystemer som Skype
- Videoløsninger/-samtalerom
- Satelittelefoner
- Nødnett
- VHF-radio

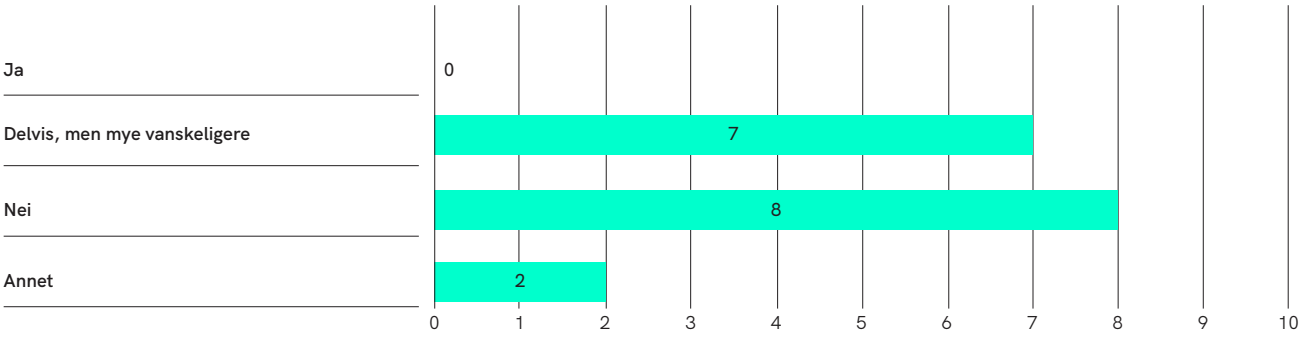
Forskjellige kombinasjoner av nødsystemer oppgis å variere etter situasjon og behov.

Virksomhetene ble spurt om når helsepersonell sist ble øvd i nødrutinene for de ulike telefoniløsningene. Svarene var:

- Ni virksomheter har ikke øvd personell i nødrutine for ulike telefoniløsninger.
- Tre virksomheter svarte at de sist øvde på nødrutinene for telefoni i 2016.
- Fem virksomheter har øvd på nødrutinene for telefoni siste to år.

Det oppgis at mobiltelefoni har en viktig rolle i beredskapsorganisasjon og nødrutiner. Mobiltelefon vil være den primære kommunikasjonskanalen når interne telefonisystemer svikter. Enkelte foretak opplyser å ha etablert doble kommunikasjonskanaler til beredskapsfunksjoner ved å bruke både interne og eksterne telefonisystemer, eller å ha rutiner for utdeling av mobiltelefoner eller håndholdte radioer. ›

*Figur 6 Sikrer nødrutinen at bakvakter kan kalles inn, også når hovedleverandørens mobilnett er ute av drift?*




Ingen foretak oppgir å ha gode nødrutiner for å kalle inn bakvakter dersom hovedleverandørens mobilnett er ute av drift. 7 foretak svarer at de delvis har rutiner for innkalling av bakvakt ved telefoniproblem. Hvis ansatte i bakvakt oppdager problemer med mobilnettet og ikke oppnår kontakt med IKT driftsleverandør, beredskapsvakter eller personell på vakt, må de selv møte opp på sykehuset. Virksomheten kan også sende bil til bostedsadresse dersom man ikke oppnår kontakt med personell med kritiske funksjoner. Enkelte foretak pålegger i den forbindelse kliniske avdelinger å ha oppdaterte papirlister med adresse for sine ansatte. Virksomhetene oppgir at rutinene kan være vanskelig å etterfølge ved svikt.

### 3.6.3 Sykesignalanlegg

Alle virksomheter har svart på spørsmål vedrørende nødrutiner for sykesignalanlegg. Sykesignalanleggene består av flere komponenter inkludert alarmsnor på pasientrom. Alarmering foregår via lyd-/lyssignal og displaypanel på korridor eller vaktrom. Alarmering videresendes hos mange virksomheter til ringesløyfe eller funksjonstelefoner i telefoni-, DECT eller personsøkersystemer. Ved manglende svar eller svar uten påfølgende kvittering på pasientrom går alarm videre til neste person i sløyfa. Hos noen medfører bortfall av telefoni at alarmering opphører, og det oppstår risiko for svikt i helsehjelp.

3 av 17 virksomheter (18 %) mangler nødrutiner for sykesignalsystem.

Som nødrutine planlegger noen å gi 'friske' pasienter bjeller, la pasienter ligge med åpne dører, øke bemanning eller føre hyppig tilsyn med pasienter som ikke kan varsle selv. ›

> «Hendelser der både IKT-nettverk og flere kommunikasjons-kanaler feiler samtidig vil bli spesielt utfordrende, noe ingen av beredskapsplanene har gode løsninger for.»

Innsendte avvik viser eksempel på at man ikke har oppnådd kontakt med personell med akuttfunksjoner ved bortfall av sykesignalsystem.

### 3.6.4 Øvelser i nødrutine for stansalarmer

9 av 17 foretak (53 %) svarer at de aldri har øvd i bruk av nødrutinen for bruk ved bortfall av stansalarmer. De resterende foretakene oppgir å ha øvd på rutinen det siste året.

### 3.6.5 Helsetilsynets refleksjoner og vurderinger av funn

**Beredskapsorganisasjon**

Virksomhetene virker å ha godt definerte beredskapsorganisasjoner med tydelige roller og avgrensninger. Beredskapsplanene kommer i tillegg til virksomhetenes nødrutiner for ulike systemer og henviser ofte til at klinikkene selv skal ha nødrutiner og beredskapsplaner for situasjonene som oppstår. Det er ikke kartlagt om klinikkene har utarbeidet slike avdelingsvise beredskapsplaner eller nødrutiner. Hendelser der både IKT-nettverk og flere kommunikasjonskanaler feiler samtidig vil bli spesielt utfordrende, noe ingen av beredskapsplanene har gode løsninger for. Samtidig øker kommunikasjonssystemenes avhengighet av IKT-nettverk sannsynligheten for slike episoder.

Den som beslutter å gå over til beredskapsdrift må kjenne til de kliniske konsekvensene for IKT-bortfall. Dette for å sikre at responsen er tilstrekkelig tilpasset typen bortfall.

I virksomhetene der AMK har en koordineringsrolle også i IKT-beredskapssituasjoner, kan det være en utfordring at bortfallet av IKT også gjør arbeidet i AMK mye mer krevende. Har de da ressurser til å takle begge oppgavene?

**Telefoni**

Bortfall av offentlige mobiltelefonitjenester kombinert med behov for kontakt med personell som ikke befinner seg på sykehuset, vil være utfordrende for alle virksomheter. Basert på hendelser rapportert i media er det ikke utenkelig at mobiltelefoni faller bort, og det bør vurderes å ha flere nødløsninger som kan gi mulighet til å kontakte eller kalle inn personell med kritiske funksjoner ved bortfall.

Telefoniløsninger er sentrale i mange ordinære kritiske arbeidsprosesser, og de er sentrale i mange nødrutiner ved sykehusene. Telefoni brukes også til å kommunisere med aktører eksternt, og bortfall får også konsekvenser eksternt. Samtidig baserer telefoniløsningene seg stadig mer på eksisterende nettverk og vil ›

kunne falle bort samtidig som andre IKT-systemer. Det er derfor betenkelig at en stor del av virksomhetene ikke har øvd personell i bruk av nødrutiner for ulike telefoniløsninger. Etablerte nødfunksjoner som bruk av Nødnett, mobiltelefoni via eksterne nett, håndholdte radioer eller liknende er derfor viktige for å kunne sikre forsvarlighet i pasientbehandlingen. Det er ukjent om nødrutinene for telefoni er i tilstrekkelig grad innført og gjort kjent ved alle relevante klinikker.

Det er registrert avvik som viser at telefonisk kontakt har feilet som nødrutine ved en av virksomhetene. Dette er en alvorlig hendelse som understreker viktigheten av gode nødrutiner også for telefoni.

**Sykesignalanlegg og stansalarmer**
Pasient- og sykesignalanlegg er kritiske systemer med høye krav til tilgjengelighet. Enkeltkomponenter i systemene er ofte frittstående, og systemene har ofte varslingsfunksjoner som baserer seg på systemer som DECT eller IP-telefoni. Bortfall av varslingsfunksjonalitet sammen med telefonisystemene kan skape utfordrende situasjoner, med høy risiko for at alvorlig syke pasienter eller helsepersonell som tilkaller hjelp ikke får rask nok støtte. Avvik viser at slike situasjoner skjer, og bare 9 av 17 (53 %) av virksomhetene oppgir å ha øvd på bruk av nødrutinen for stansalarmer. Nødrutinene kan innebære oppbemanning eller andre tiltak som krever kommunikasjon utover avdelingen i en situasjon med mulig bortfall av telefoni. Dette understreker igjen viktigheten av å ha etablert gode alternative kommunikasjonskanaler, samt å øve på å bruke de i praksis.

## 3.7 Nødrutiner som gjelder ved bortfall av IKT er kjent i virksomheten og oppdateres ved behov

### 3.7.1 Kjennskap til nødrutiner hos ansatte

Virksomhetene ble bedt om å oppgi hvordan nyansatte sykepleiere og leger blir gjort kjent med virksomhets nødrutiner. 8 av 17 virksomheter (47 %) oppgir at alle nyansatte får kurs eller opplæring i nødrutinene. 7 virksomheter (41 %) oppgir at mengden opplæring som gis varierer, og 2 virksomheter (12 %) oppgir at bare noen nyansatte får opplæring i nødrutiner.

Virksomhetene ble også spurt om hvordan kunnskap om nødrutinene blir vedlikeholdt i organisasjonen. Flere virksomheter oppgir å ha varierende praksis, og mange bruker flere metoder for å opprettholde kompetanse. 9 av 17 virksomheter (53 %) oppgir å alltid gi informasjon til ansatte ved vesentlige oppdateringer av rutinene. 5 av 17 ›

«15 foretak (88 %) oppgir at nødrutiner er tilgjengelig i papirformat på alle kliniske avdelinger.»

virksomheter (29 %) oppgir at rutiner distribueres ved planlagt nedetid, og 4 av 17 virksomheter (24 %) vedlikeholder kompetanse ved å avholde kurs.

### 3.7.2 Plassering/tilgang og jevnlig forbedring av nødrutiner

15 foretak (88 %) oppgir at nødrutiner er tilgjengelig i papirformat på alle kliniske avdelinger. 2 foretak (12 %) lagrer nødrutiner på lokale PC-er ved alle kliniske avdelinger og papirutskrifter ved noen avdelinger. Det er ikke undersøkt hvilken avstand ulike sengeposter eventuelt har til papirrutinene, eller om personellet er kjent med hvor disse permene er.

14 foretak (82 %) svarer at nødrutinene oppdateres jevnlig etter øvelser, større oppgraderinger, andre behov, eller ved forhåndsdefinerte tidsintervaller. 3 foretak (18 %) har ingen rutiner for å oppdatere nødrutinene.

Enkelte virksomheter har sendt inn retningslinjer for hvordan man arbeider med nødrutiner i virksomheten. Sentralt i disse retningslinjene er «beredskapspermer», som skal oppbevares på de ulike avdelingene. Beredskapspermene inneholder papirark med aktuelle nødrutiner for kliniske IKT-system. Det utpekes en person ved hver avdeling (ofte leder) som har ansvar for at permen er tilpasset de lokale forhold, og at permen til enhver tid er oppdatert. Den ansvarlige personen skal også holde oversikt over hvem som har mottatt informasjon om permen og de lokale nødrutiner for den enkelte avdelingen. Dette for å sikre at alle ansatte kjenner til innholdet og vet hva de skal gjøre om det blir driftsstans. Følgende sitat belyser hvordan dette arbeidet forgår ved en av virksomhetene: «Alle blanketter som benyttes ved seksjonen og som er tilgjengelig elektronisk i DIPS, skal ligge i papirform med nødprosedyrer».

### 3.7.3 Bruk av avviksrapporter i forbedringsarbeid

16 av 17 forespurte helseforetak (94 %) har sendt inn oversikter over avvik i pasientbehandlingen forårsaket av IKT-utfordringer. Det er i alt sendt inn 639 avvik som er knyttet til IKT. Oversiktene fra flere virksomheter er lite detaljerte og det er ikke alle virksomheter som har strukturert avvikene i ulike kategorier. Det er sendt inn varierende mengde og type opplysninger om de registrerte avvikene knyttet til IKT.

Av de kategoriserte avvikene er 89 avvik (14 %) kategorisert som treghet i eller bortfall av IKT-systemer. Tallet inkluderer også svikt i telefoni- og varslingssystemer, samt stans i dataflyt mellom forskjellige systemer. 11 % av alle kategoriserte avvik er relatert til bruk av kurvesystemer, ›

registrert ved 5 virksomheter. Gjennomsnittlig er over 23 % av avvikene ved disse 5 virksomhetene vedrørende kurvesystemer. Ved en virksomhet er 44 % av IKT-avvikene vedrørende elektronisk legemiddelkurve.

Dårlig brukervennlighet og svake grensesnitt i IKT-systemer er årsaker til hendelser som blant annet manglende innkalling, feilmedisinering og reoperasjoner. Kategorisering av avvikene varierer noe mellom brukervennlighet, brukerfeil og opplæring. Manglende systemtilgang er også gjengangere i registrerte IKT-avvik. Svikt i manuelle rutiner, prosedyre- eller retningslinjer rundt bruk av IKT-systemer er også meldt ved noen foretak. Flere saker med mangelfull eller uklar prosedyre som årsak kan også settes i sammenheng med dårlig brukervennlighet.

13 av 17 virksomheter (76 %) oppgir at avvik og endringsønsker meldes til IKT-leverandør når det er aktuelt, og de fleste foretakene svarer at de har rutiner for oppfølging av disse sakene. Mer alvorlige saker kan også bli eskalert til egne oppfølgingsmøter med IKT-leverandør. Fire foretak oppgir at IKT-driftsleverandør ikke får informasjon om IKT-relaterte avvikssaker med mindre helsepersonellet selv melder feilen til denne, noe som forutsetter at IKT-brukeren dobbeltregistrerer sak.

På spørsmål om hvem som holder oversikt over IKT-relaterte avvikssaker knyttet til forsvarlig helsehjelp svarte 15 av 17 virksomheter (88 %) at helseforetaket gjør det. To svarte at IKT-driftsleverandøren gjør det.

### 3.7.4 Oppfølging av IKT-feil som er viktige for pasientsikkerhet

Det varierer om helseforetakene følger opp at IKT-feil som er meldt til IKT-driftsleverandør blir fulgt opp ihht risiko knyttet til pasientsikkerhet.

*Tabell 3 Helseforetakene sin oppfølging av saker meldt til IKT-leverandør*

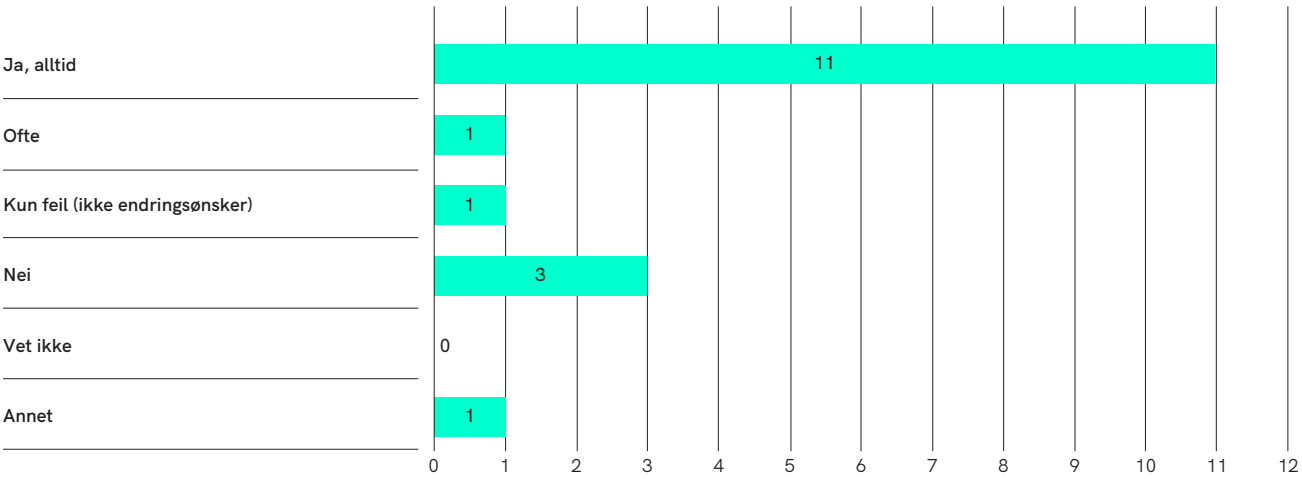
| | Svar | |
|---|---|---|
| Vi (helseforetaket) følger opp alle feil knyttet til pasientsikkerhet blir rettet av IKT-driftsleverandør | 47,06 % | 8 |
| Annet (vennligst spesifiser) | 35,29 % | 6 |
| Det varierer om vi (helseforetaket) følger opp at feil/endringsønsker blir rettet av IKT-driftsleverandør | 17,65 % | 3 |
| Vi (helseforetaket) følger sjelden opp feilretting av enkeltsaker meldt til IKT-driftsleverandør | 00,00 % | 0 |
| Ingen saker blir fulgt opp fra helseforetaket | 00,00 % | 0 |
| **Totalt antall respondenter** | | 17 |

Helseforetakene oppgir ulike grunner for at de ikke kan følge opp prioritering av saker hos egen IKT-leverandør. Vanligste årsak er manglende informasjon om hvilke saker som er meldt fra brukere ved sykehuset til IKT-driftsleverandøren. Foretakene mangler innsyn i IKT-leverandørens sakssystemer og får ikke tilstrekkelige oversikter over hvilke saker som er meldt til IKT-kundesenter fra eget helseforetak. Kommentar fra en virksomhet er:

«Enkeltsaker meldt av bruker direkte til driftsleverandøren følges ikke opp av foretaket, med mindre driftsleverandøren melder dette tilbake som feil med behov for oppmerksomhet».

Det er 11 av 17 virksomheter (65 %) som svarer at IKT-feil som meldes til IKT-kundesenteret blir fulgt opp, etter vurdering av pasientsikkerhet.

*Figur 7 Blir IKT-feil som er meldt til IKT-driftsleverandør sitt kundesenter kategorisert, prioritert og fulgt opp ihht risiko knyttet til pasientsikkerhet?*




Virksomhetene ble bedt om å sende oversikter over de mest risikofylte feil/endringsønsker som IKT-driftsleverandør har registrert, dato for innrapportering og relevante tidfestede tiltak. Det er sendt inn 7 oversikter over tidligere feilsituasjoner og en oversikt over pågående IKT-saker. Det er ikke sendt inn noen planer for utbedring av pågående IKT-feil eller endringsønsker.

### 3.7.5 Helsetilsynets refleksjoner og vurderinger av funn

**Kjennskap til nødrutiner hos ansatte**

Det er variasjon på hvor mye opplæring sykepleiere og leger får i nødrutinene i virksomhetene. Mange foretak sikrer ikke at nødrutinene systematisk blir oppdaterte, eller at opplæring blir gjennomført. I

praksis gjør hyppige situasjoner med bortfall at nødrutinene blir innarbeidet i klinikkene.

Bortfall av kritiske systemer, for eksempel EPJ, kurveløsning eller pasientovervåkning, kan kreve arbeidsintensive manuelle nødrutiner. Det er derfor viktig at ledelsen arbeider systematisk for å sikre at kvaliteten på nødrutiner er i samsvar med forsvarlighetskrav, og at personellet har fått tilstrekkelig opplæring. Å forvente at helsepersonell jevnlig leser oppdaterte nødrutiner i et kvalitetssystem er neppe tilstrekkelig for systemer med høy oppetid og sjeldne reelle «øvelser». Det å bruke tid på å lete i kvalitetssystem i akutte situasjoner er uheldig bruk av kritisk tid og risikabel praksis fordi kvalitetssystemene også kan være ute av funksjon. For systemer som brukes til overvåkning av kritisk syke pasienter, ser vi at nødrutinene består i oppbemanning. I perioden frem til ekstra personell har ankommet, må de som er på vakt både overvåke pasientene og selv kalle inn ekstra ressurser. Dette er konkurrerende aktiviteter som kan få følger for oppmerksomhet til kritisk syke pasienter.

Helsepersonell har i kartleggingsarbeidet pekt på behov for enkle nødrutiner, der en benytter verktøy som er kjent. Selv om en har øvd på bruk av radio kan det i akutte situasjoner være vanskelig å huske hvor telefonnummer er lagret og hvodan nye verktøy fungerer.

Siden virksomhetene har færrest øvelser i nødrutiner knyttet til ulike typer alarmer og telefoner, bør alle vurdere bruk av simulering for kompetanseheving.

De regionale helseforetakene har fått et generelt oppdrag fra HOD om å øke bruk av simulering for kompetanseheving, og samarbeide med andre helseforetak om utvikling og deling av opplegg for simulering.

**Plassering/tilgang og jevnlig forbedring av nødrutiner**

Papirkopier av nødrutinene blir i de fleste virksomheter oppbevart i en beredskapsperm ved klinikkene. Virksomhetene virker for det meste å ha godt innarbeidede rutiner for å gjøre kjent hvor permen befinner seg, samt et etablert ansvar for å holde permene oppdaterte ved vesentlige endringer.

Flere foretak oppgir som nevnt, at nødrutinene i tillegg befinner seg i interaktive kvalitetssystemer. Disse systemene vil også kunne bli berørt av IKT-bortfall, som da vil medføre at nødrutinene blir utilgjengelige for brukerne. Virksomhetene bør vurdere risikoen ved bruk av slike systemer, og sikre at alle nødrutiner med kritiske telefonnummer og lignende er tilgjengelig lokalt ved bortfall av nettverk. ›

> «Kartleggingen viser at det er varierende praksis for registrering av uønskede pasienthendelser på grunn av mangler eller feil i IKT-system i de ulike virksomhetene.»

### Bruk av avviksrapporter i forbedringsarbeid

Det er usikkert i hvilken grad forbedringsforslag og avvik fører til endringer i rutiner og IKT-systemer. Mange helseforetak hevder at de følger opp retting av avvik hos IKT-levererandører. Helsetilsynet har behandlet saker der dette ikke er gjort.

Kartleggingen viser at det er varierende praksis for registrering av uønskede pasienthendelser på grunn av mangler eller feil i IKT-system i de ulike virksomhetene. At avvik ikke meldes, kan handle om at ansatte ikke har kunnskap eller forståelse for hensikten med å melde avvik, ikke får vite hvordan avviket blir fulgt opp, eller at det mangler arenaer for felles gjennomgang for å sikre organisatorisk læring (10). Norsk Pasientskadeerstatning (NPE) peker også på behov for bedre avviksregistrering (6):

«I dette materialet ser vi eksempler på flere saker med alvorlige konsekvenser for pasienten, som ikke er funnet igjen i avvikssystemet […] Når samsvaret er så lavt, er det en fare for at det lokale avvikssystemet ikke gir et godt nok bilde av type skader som betyr mest for pasientene. Dette påvirker læringsgrunnlaget sykehusene har for å lære av feilene og unngå at de skjer i fremtiden.»

Det er uheldig at verken IKT-ledere eller helsefaglig ledelse har det fulle bildet over avvik og risiko i pasientbehandlingen grunnet IKT. IKT-feil meldes ofte bare til IKT-driftsleverandør, helseforetakene mangler tilgang til meldte saker og viktige IKT-utfordringer blir oversett i kvalitetsarbeidet.

I denne kartleggingen har helsepersonell også nevnt behov for felles logg, forum for læring og deling av erfaringer knyttet til IKT-bortfall ved ulike helseforetak i Norge.

### Oppfølging av IKT-feil som er viktige for pasientsikkerhet

Det har kommet frem at virksomhetene mangler oversikt over hvilke saker som er meldt IKT-driftsleverandørene og dermed hvilke risiko sakene har for pasientbehandlingen. Dette gjør det vanskelig for sykehusene å følge opp systematisk, lovpålagt forbedringsarbeid.

Sluttbrukere melder feil og endringsønsker til IKT-driftsleverandør, som prioriterer sakene etter kriterier i SLA. Prioriteringen gjøres blant annet etter hvor kritisk en har definert systemet og hvor mange brukere feilen berører. Retting av konkrete feil prioriteres normalt høyere enn endringsønsker. En utfordring i dette er for eksempel at det som klassifiseres som et endringsønske, kan for innmelder oppleves som en feil som gir betydelig økt risiko i pasientbehandlingen. En sak som omhandler brukervennlighet i et medikamentsystem vil for eksempel ›

> «De innsendte avvikene viser at det er registrert feil i IKT-systemene som har ført til dødsfall og andre pasientskader.»

kunne klassifiseres som et endringsønske og dermed nedprioriteres av IKT-driftsleverandør (og underleverandør). Sagt på en annen måte vil mål om forsvarlig helsehjelp i noen tilfeller konkurrere med SLA-krav. Helseforetakene har ansvar for forbedringsarbeid, men mangler systematiske oversikter over slike saker.

Foretakene har ikke innsikt i hvilke saker IKT-driftsleverandøren har registrert, og er derfor avhengige av at vurdering av hvilke saker som kan medføre risiko avgjøres av en IKT-driftsleverandør. Et slikt skille mellom ansvar og tilgang til informasjon er ikke hensiktsmessig fordi vurdering av risiko vil kreve helsefaglig kompetanse. IKT-driftsleverandørene bør derfor gi helseforetakene full innsikt i alle registrerte saker.

Virksomhetene ble bedt om å sende oversikter over både avvik og de mest risikofylte feil/endringsønsker som IKT-driftsleverandør har registrert og relevante tidfestede tiltak. Det er ikke sendt inn noen planer for utbedring av pågående IKT-feil eller endringsønsker. Kartleggingen viser at helseforetakene mangler systematisk oversikt over hvilke IKT-saker som har størst konsekvens for forsvarlig helsehjelp og pasientsikkerhet. De innsendte avvikene viser at det er registrert feil i IKT-systemene som har ført til dødsfall og andre pasientskader. Det er derfor bekymringsfullt at ingen virksomheter har sendt inn planer for utbedring av pågående IKT-feil eller endringsønsker. Dette er ikke i tråd med forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten.

## 3.8 Styringsmodell for IKT

### 3.8.1 Kort om beslutningsstruktur

Virksomhetene ble spurt om hvilken informasjon og beslutningsstruktur som gjelder vedrørende etablering av lesekopi av EPJ ved IKT-bortfall. Fire virksomheter krysset av for at de blir informert om alle risikofylte endringer og kan bestille lesekopi ved behov. Alle virksomheter svarte at de er delaktige i dialog med IKT-driftsleverandør om når lesekopi skal settes opp. Dialogen med å etablere lesekopi ved oppståtte feil varierer noe. Ved akutte kriser benyttes ofte beredskapsledelsen, og for øvrig går dialogen ofte gjennom regionale og lokale EPJ-senter.

For å belyse styringsmodeller for IKT ble det videre spurt om helseforetakene sine roller ved oppgradering av EPJ-systemet. 16 av 17 virksomheter (94 %) svarte at de hadde deltatt i utarbeiding av risikoanalyser av oppgraderinger av EPJ. Det er ikke undersøkt hvilken kompetanse, mandat eller rolle disse deltagerne hadde i utarbeidingene.

> «Kartleggingen viser at de regionale helseforetakene ikke har klargjort ansvarsfordeling og organisering mellom IKT-driftsleverandører og helseforetak tilstrekkelig for å sikre samarbeid, systematisk styring og forbedring.»

12 av 17 virksomheter (71 %) svarte at fagdirektør hadde godkjent restrisikoen for oppgradering av DIPS/DocuLive. I ett foretak var det adm.dir. som hadde godkjent restrisiko og for øvrige foretak var det lagt inn kommentarer med lignende løsninger, men også regionale utvalg var nevnt som beslutningsorgan for oppgraderinger.

### 3.8.2 Helsetilsynets refleksjoner og vurderinger av funn

Det er positivt at ledelsen ved helseforetak blir forelagt beslutninger om oppgradering av EPJ. Det er en svakhet at bare 5 av 17 virksomheter (29 %) blir informert om alle risikofylte IKT-endringer og derfor kan vurdere om lesekopi av EPJ skal bestilles i forkant av risikofylte endringer. De som bestiller lesekopi av EPJ i forkant av feil sparer 15-90 minutter nedetid dersom EPJ feiler. Det er som tidligere nevnt, også påfallende at overordnede risikoanalyser for IKT-bortfall jevnt over ikke inneholder vurderinger av konsekvenser av IKT-bortfall. Helsetilsynet ser dette som svakheter i styringsmodellen. Dette er tegn på at det juridiske ansvaret foreløpig er for uklart flere steder, og at manglende ansvarsavklaring igjen medfører fare for ulike typer svikt. Ansvaret synes å være best avklart i Helse Sør-Øst og Helse Midt-Norge der virksomhetene sender inn beskrivelser av ansvarsfordeling. Det fremstår likevel som uklart også her om helseforetakene har fulgt opp ansvaret for å sikre forsvarlig beredskap og helsehjelp godt nok.

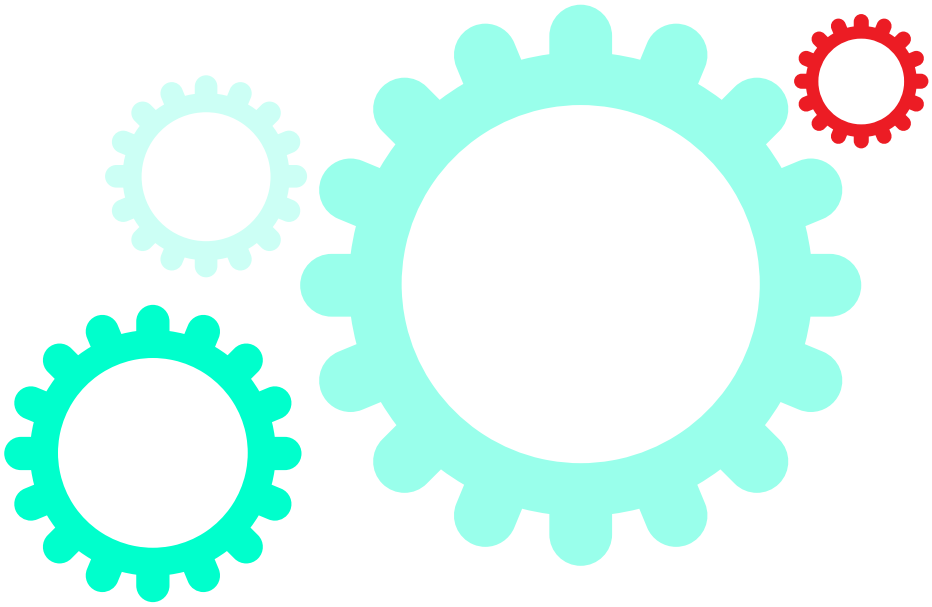
Dersom nettverket feiler, er det som nevnt bare to virksomheter som har nødløsning for tilgang til EPJ for nye pasienter. Ut fra gjeldende styringsmodell burde virksomhetene være informert om alle risikofylte endringer for å kunne vurdere tiltak og forebygging. Det bør gjøres endringer i styringsmodellen, og helseforetakene må vurdere tilgang til EPJ-opplysninger ved alle akuttmottak ved IKT-bortfall. Nedetid ved planlagte endringer bør også holdes til et minimum, og legges til perioder som påvirker pasientbehandlingen i minst mulig grad. Kartleggingen viser at ansvarsfordeling og organisering mellom IKT-driftsleverandører og helseforetak ikke er tilstrekkelig klargjort for å sikre samarbeid, systematisk styring og forbedring.

Det er en svakhet i kartleggingen at det ikke ble sendt inn og vurdert mer dokumentasjon om risikoanalyser av forsvarlig helsehjelp knyttet til endring av funksjoner i EPJ. Virksomhetene har i svært liten grad lagt frem overordnede risikoanalyser der IKT-saker er vurdert opp mot pasientsikkerhet eller forsvarlig helsehjelp. Det er vår oppfatning at helseforetakene oftest deltar i testing og vurdering av nye funksjoner i kritisk programvare som skal innføres ved foretaket. Fagdirektører er ofte utpekt som systemeiere for EPJ og blir informert/involvert om EPJ-endringer. Fagdirektørene er avhengig av et tilstrekkelig kompetent ›

støtteapparat rundt seg for å vurdere EPJ-endringer og risiko. Dette er ikke kartlagt eller vurdert i undersøkelsen.

Risikoanalyser, nødrutiner, godt samspill og tydelig ansvarsfordeling er vesentlig for god sikkerhetsstyring i virksomhetene. Det er et tydelig forbedringspotensiale å avklare og tydeliggjøre roller og ansvar for sikkerhetsstyring i virksomhetene, som beskrevet over. Når IKT-personell gjør en prioritering av feil basert på kriterier i SLA, kan det som nevnt motstride prioritering i forhold til forsvarlig helsehjelp. For å sikre at viktig informasjon om uønskede hendelser og sårbarheter tas med i risikovurderinger, er det også viktig å ha gode kvalitetssystemer på plass. Det er en ulempe at virksomheter har registrert IKT-feil i et system hos IKT-driftsleverandør, og at helseforetakene ikke har innsyn i innrapporterte feil fra egen virksomhet. Dette er et eksempel på lange verdikjeder, som også Helsedirektoratet identifiserer som en risiko for helse- og omsorgssektoren (18).

Helsepersonell opplever det som uhensiktsmessig å dobbeltrapportere IKT-feil som har ført til pasientskader i interne avvikssystem. Kombinert med varierende meldingskultur (6) ser dette ut til å føre til en del manglende avviksrapportering. Arbeidet med å yte helsehjelp er nå så tett forbundet med IKT-systemer, at arbeid med å redusere risiko og håndtere uønskede hendelser må skje i fora der representanter fra både den kliniske virksomheten og IKT-ledelsen er med. Styringsorganene må ha gode styringsdata uten å belaste helsepersonell med unødvendig dobbeltregistrering. ●



# 4

# Litteraturliste


1. Hvordan er sykehusene forberedt på IKT-bortfall? Rapport fra Helsetilsynet 3/2020. Oslo: Statens helsetilsyn, 2020.
2. Utfører dataangrep og krever løsepenger: Sykehus er populære mål. TV2.no 14.02.21.
3. Undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer Rapportvedlegg til Dokument 3:2 (2020-2021). Oslo: Riksrevisjonen, 2020.
4. Hansen, E. Tekniske katastrofer – hva gjør man når systemene svikter? Foredrag på konferansen Helsetjenesten under angrep, 6. juni 2019. NSH - Norsk sykehus- og helsetjenesteforening.
5. Varsel om vedtak – overtredelsesgebyr – Sørlandet Sykehus HF. Brev fra Datatilsynet til Sørlandet sykehus HF, 24.10.2017. (Ref. Datatilsynet 16/01531-45/GRA) 007-2018.
6. Undersøkelse av samsvar mellom NPE-saker og saker i sykehusenes meldesystemer. Rapport meldesystem 2014-2017. Oslo: NPE, 2020.
7. Meld. St. 38 (2016–2017). IKT-sikkerhet – Et felles ansvar.
8. Meld. St. 9 (2012-2013). Én innbygger – én journal.
9. Prop. 1 S (2020–2021). Helse- og omsorgsdepartementet.
10. Meld. St. 11 (2020-2021). Kvalitet og pasientsikkerhet 2019.
11. Seip ÅA. Sourcingstrategier for IKT i offentlig sektor. Fafo-rapport 2020:17. Oslo: Fafo, 2020.
12. Utviklingstrekk 2020. Drivere og trender for e-helseutviklingen. Oslo: Direktoratet for e-helse, 2020.
13. UNN skulle oppdatere systemet for pasientjournalene – må utsette flere operasjoner, NRK 10. feb. 2020.
14. Kritiske datasystemer på vei opp i Helse Sør-Øst, VG 18. januar 2019.
15. Sensitiv pasientinformasjon kan være på avveie etter dataangrep. NRK 10. januar 2021.
16. Østre Toten har vært uten datasystem en måned etter hacking. NRK 8. februar 2021.
17. Situasjonsbilde 2018. Oslo: HelseCERT/Norsk helsenett, u.å.
18. Overordnede risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren. Rapport 06/2017. IS-2635. Oslo: Helsedirektoratet, 2017.
19. Læring for bedre beredskap. IS-1984. Oslo: Helsedirektoratet, 2012.
20. Nødnett. Helsedirektoratet.
21. Hydro er fortsatt ikke friskmeldt etter dataangrepet i mars. Digi.no 8. mai 2019.
22. Schopf T et al. How well is the electronic health record supporting the clinical tasks of hospital physicians? BMC Health Serv Res 2019; 19: 934.
23. Nilsen L. Videomøte med fastlegen var i halvparten av tilfellene like bra som time på legekontoret. Forskning.no, 21. februar 2021.
24. Digital hjemmeoppfølging ved covid-19. Oslo: Helsedirektoratet, 2021.
25. Befolkningens helsekompetanse. Oslo: Helsedirektoratet (sist faglig oppdatert 25. januar 2021, lest 29. januar 2021).
26. Akuttmedisinsk informasjonssystem - AMIS, administrative data ved Helse Stavanger.

27. Behandlingsansvarlig og databehandler. Datatilsynet.

28. E-konsultasjoner utenfor vanlig arbeidstid. Helsedirektoratet.

29. Pasientjournal,Volven. Direktoratet for e-helse.

30. Elektronisk pasientjournal. Wikipedia

31. PACS. Store medisinske leksikon.

32. RIS. Store medisinske leksikon.

33. Hva er risikovurdering? Digitaliseringsdirektoratet.

## Øvrige kilder og litteratur

EPJ standard. Tilgangsstyring, retting og sletting. (Teknisk standard nr. HIS 80506:2019.) Oslo: Direktoratet for e-helse, 2019.

Iverksette styringssystem for informasjonssikkerhet. Datatilsynet

LOV-2020-12-18-145. Lov om helsemessig og sosial beredskap (helseberedskapsloven).

Meld. St. 27 (2015-2016). Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet.

Metodebibliotek for IKT-arbeid i spesialisthelsetjenesten Kilden.

Nasjonal strategi for informasjonssikkerhet. Oslo: Justis og beredskapsdepartementet, Forsvarsdepartementet, 2019.

Faktaark 11 – Nødprosedyrer ved bortfall av IKT Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.

Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen). Versjon 6.0. Vedtatt 4. februar 2020, Direktoratet for e-helse.

Overordnede risiko- og sårbarhetsvurderinger for nasjonal beredskap i helse- og omsorgssektoren 2019. Rapport IS-2841. Oslo: Helsedirektoratet, 2019.

Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack. The New York Times

NOU 2012:14. Rapport fra 22. juli-kommisjonen.

Risikoanalyse. Hendelsesanalyse: Håndbok for helsetjenesten. IS-0583. Oslo: Helsedirektoratet, 2019.

Sleveland A. Forsvarlighet og sikkerhet på sykehusene. En analyse av 20 tilsynsrapporter hos Statens helsetilsyn. Masteroppgave. Stavanger: Universitetet i Stavanger, 2020.

Veileder i planlegging, gjennomføring og evaluering av øvelser – grunnbok. Tønsberg: Direktoratet for samfunnssikkerhet og beredskap, 2016.

EPJ standard. Tilgangsstyring, retting og sletting. (Teknisk standard nr. HIS 80506:2019.) Direktoratet for e-helse, 2019.

Iverksette styringssystem for informasjonssikkerhet. Datatilsynet, Lest 1.1.2020.

LOV-2020-12-18-145 Lov om helsemessig og sosial beredskap (helseberedskapsloven)

Meld. St. 27 (2015-2016) Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet

Metodebibliotek for IKT-arbeid i spesialisthelsetjenesten - Kilden Lest 1.1.2020.

Nasjonal strategi for informasjonssikkerhet. Fornyings-, administrasjons-, og kirkedepartementet, 2012.

Faktaark 11 – Nødprosedyrer ved bortfall av IKT Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren

Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen). Versjon 6.0. Vedtatt 4. februar 2020.

Overordnede risiko- og sårbarhetsvurderinger for nasjonal beredskap i helse- og omsorgssektoren 2019. Rapport IS-2841.Helsedirektoratet, 2019.

Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack - The New York Times (nytimes.com) (lest 27.11.20)

Rapport fra 22. juli-kommisjonen, NOU 2012: 14. regjeringen.no

Risikoanalyse. Hendelsesanalyse: Håndbok for helsetjenesten. IS-0583. Helsedirektoratet, 2019.

Sleveland, Anette. Forsvarlighet og sikkerhet på sykehusene. Universitetet i Stavanger, 2020.

Veileder i planlegging, gjennomføring og evaluering av øvelser – grunnbok. DSB 978-82-7768-385-0, 2016.


# 5

# Vedlegg



## 1. Ordliste, begrepsbruk

**AMIS – Akuttmedisinsk informasjonssystem** IKT-støtteverktøy som benyttes ved akuttmedisinske kommunikasjonssentraler, legevaktsentraler og ambulansetjenesten. Benyttes til mottak og registrering av nødmeldinger, bestilling av ambulansetransport, koordinering og prioritering av oppdrag, pasientoversikt og ambulansejournal. (26)

**Behandlingsrettet helseregister** Journal- og informasjonssystem eller annet helseregister som har til formål å gi grunnlag for handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte pasient og som utføres av helsepersonell, og administrasjon av slike handlinger.

**Bortfall av IKT-system** Brukere opplever at ett eller flere IKT-system de vanligvis benytter i sin arbeidssituasjon ikke er tilgjengelige. Det kan f.eks. være at systemet ikke lar seg starte, at brukere ikke får logget på selv om det oppgis korrekt autentisering eller at treghet eller feil i systemet gjør det umulig å benytte.

**Dataansvarlig** Dataansvarlig er den som bestemmer formålet med behandlingen av helse- og personopplysningene og hvilke hjelpemidler som skal brukes, hvis ikke dataansvaret er særskilt angitt i loven eller i forskrift i medhold av loven, jf. helseregisterloven § 2 nr. 8 og personvernforordningen artikkel 4 nr. 7 (her benyttes begrepet" behandlingsansvarlig"). Det presiseres at det er virksomheten som er dataansvarlig for behandling av helse- og personopplysninger. Ansvaret skal ivaretas av den daglige ledelsen av virksomheten, og virksomheten er pliktsubjekt. (27)

**Databehandler** Databehandler er den som behandler helse- og personopplysningene på vegne av den dataansvarlige, jf. Personvernforordningen artikkel 4 nr. 8.

**E-konsultasjon** E-konsultasjon er et samlebegrep for de digitale konsultasjonsformene tekstkonsultasjon og videokonsultasjon. E-konsultasjonen må inneholde en medisinsk vurdering eller samtale. Fra mars 2020 ble det også mulig å benytte telefon ved e-konsultasjon. (28)

**Elektronisk medikasjons- og kurveløsning** Elektronisk løsning for håndtering av medikasjon, og fremstilling av essensielle pasientdata som for eksempel fysiologiske målinger som puls, blodtrykk og temperatur. Kan også inneholde informasjon om behandling som for eksempel oksygentilskudd, ventilasjon, væske og bruk av blodprodukter.

**EPJ – Elektronisk pasientjournal** Elektronisk ført samling eller sammenstilling av nedtegnede/registrerte opplysninger om en pasient i forbindelse med helsehjelp (29,30). En pasients samlede journal kan bestå av opplysninger som befinner seg i flere forskjellige EPJ-system.

**Fagsystem** En applikasjon eller et IKT-system som behandler helse- og personopplysninger og som benyttes i pasientbehandlingen. Begrepet systemløsning brukes også om et fagsystem. Eksempler på fagsystem er: pleie- og omsorgssystem, legekontorsystem og barnevernsystem. Opplysninger i ulike fagsystem kan både utgjøre elektronisk pasientjournal (EPJ) og annen tjenestedokumentasjon.

**IKT-sikkerhet /informasjonssikkerhet** Integritet, konfidensialitet og tilgjengelighet er viktige sikkerhetsmål når det gjelder å ivareta IKT-sikkerhet. ›

- Konfidensialitet innebærer at informasjon ikke avsløres for uvedkommende, og at kun autoriserte personer får tilgang til den.
- Integritet innebærer at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig og et resultat av autoriserte og kontrollerte aktiviteter.
- Tilgjengelighet innebærer at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov. (7)

**IKT-system/ IT-system** Programvare og digitale tjenester som er anskaffet eller utviklet for å direkte understøtte arbeidsoppgaver i virksomheten eller som virksomheten har ansvaret for.

**Klinisk IKT-system** Et elektronisk behandlingsrettet helseregister.

**Konfidensialitet** Krav om konfidensialitet innebærer at informasjon ikke blir kjent for uvedkommende (ikke-uautoriserte personer, enheter eller prosesser).

**Kritiske IKT-system** IKT-system som ved bortfall kan utsette pasienter for unødig skade eller risiko for skade, eller på annen måte hindre forsvarlig drift av virksomheten.

**Lesekopi av EPJ** Tilgang til å lese journal elektronisk selv om 'vanlig' EPJ med skrivetilgang ikke fungerer.

**Nedetid** Utilgjengelig IKT-tjeneste, IKT-bruker sin opplevelse av at IT-tjenesten ikke fungerer.

**Nødrutiner** I dette dokumentet brukt som en samlebetegnelse for de rutiner, planer og prosedyrer som virksomheten har for å håndtere situasjoner med bortfall av IKT.

**Oppetid** Tid system er tilgjengelig for bruker av systemet

**PACS** Picture Archiving and Communication System. PACS er et elektronisk system for digital lagring, gjenfinning, visning og overføring av bilder. Systemet er i første rekke utviklet for bildediagnostikk i radiologiske avdelinger. PACS er plassbesparende og muliggjør elektronisk overføring av bildediagnostiske undersøkelser som røntgenbilder, CT, MR, ultralyd og nukleærmedisinske undersøkelser, til mottagere i andre avdelinger og sykehus (31).

**Radiologisystem** Brukes her som samlebetegnelse for RIS/PACS

**PAS** Pasientadministrativt system

**RIS** Radiology information system. 'Radiologisk informasjonssystem' er et nettbasert system for administrasjon og håndtering av pasientinformasjon knyttet til radiologiske undersøkelser (32).

**Risikoanalyse** Risikoanalyse er et verktøy som benyttes for å skaffe seg oversikt over risiko på en systematisk måte (33)

**Risikostyring** Rutiner for å identifisere, analysere, vurdere og eliminere årsaker eller omstendigheter som kan føre til pasientskade samt for å konstruktivt bruke erfaringer.

**Risikovurdering** Risikovurdering er et begrep i risikostyringen som dekker de tre stegene risikoidentifisering, risikoanalyse og risikoevaluering (33)

**SLA (Service Level Agreement)** Tjenestenivåavtale (brukes for å regulere IKT-leveranser fra regionale IKT-selskap til virksomheter). ›

**Sourcing** Sourcing handler om å hente ressurser fra ulike steder og benyttes i vanlig tale om å produsere tjenester selv eller kjøpe tjenester ute. Insourcing og outsourcing handler om å flytte tjenester inn i virksomheten eller ut av virksomheten. En sourcingstrategi kan dermed defineres som en plan for hvilke tjenester virksomheten skal produsere selv med egne ansatte, og hvilke tjenester som skal kjøpes inn fra eksterne leverandører.

**Store IKT-endringer** IKT-endringer som kan ha store konsekvenser, dvs. IKT-endringer som kan eller vil ha store konsekvenser for virksomhetens drift. Eksempler: Innføring av større kliniske IKT-system, oppgraderinger med innføring av ny funksjonalitet, endring i viktige konfigurasjonsparametere, liten endring i sentral maskinvare eller nettverks-infrastruktur som kan ha stor påvirkning på kritiske applikasjoner.

**Systemeier** Leder som er ansvarlig for å utvikle, forvalte og drifte et informasjonssystem.

**Systemforvalter** Person systemeier har pekt ut som operativt ansvarlig for oppfølging av delegerte oppgaver knyttet til et informasjonssystem, arbeider på delegasjon/ på vegne av systemeier.

**Transmed** IKT-system for flåtestyring og kartverk som brukes av akuttmedisinsk kommunikasjonssentral.

**Tilgjengelighet** Krav om tilgjengelighet innebærer at informasjon skal være tilgjengelig og anvendelig når den autoriserte ber om det.

**Øvrige definisjoner** se Norm for informasjonssikkerhet
https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren#6.1%20Definisjoner

Oslo universitetssykehus

Prosedyre

# Faglig vurdering av videokonsultasjon før oppstart med pasient

Fellesdokumenter - nivå 1 - OUS/Ledelsessystem/Informasjonssikkerhet

| Dokument-ID: 137648<br>Versjon: 0<br>Status: Godkjent | Dokumentansvarlig:<br>Lise Solberg Nes<br>Utarbeidet av:<br>Christine Rygg, Lise Solberg Nes m.fl | Godkjent av:<br>Hilde Myhren | Godkjent fra:<br>28.04.2020 |
|---|---|---|---|

## 1. Hensikt og omfang

Hensikten er å kvalitetssikre faglig forsvarlig planlegging, gjennomføring og avslutning av polikliniske videokonsultasjoner. Dette inkluderer en faglig vurdering om hvorvidt videokonsultasjon er egnet for den enkelte pasient og for formålet med videokonsultasjonen.

Med «videokonsultasjon» menes at helsepersonell og pasient ikke er i samme rom og det ytes helsehjelp ved bruk av lyd og videooverføring. Det understrekes at det med begrepet «videokonsultasjon» henvises til direkte konsultasjoner via sikker videokonsultasjonsløsning hvor samtaler er kryptert ende til annen (viser til prosedyren Forvaltning av Confrere i OUS - ehåndbok #136856), og hvor det ikke gjøres opptak eller lagring av samtalen.

Det journalføres i DIPS at helsehjelpen er gitt ved videokonsultasjon. Relevante og nødvendige opplysninger om helsehjelpen og om pasientens tilstand dokumenteres på vanlig måte i DIPS.

## 2. Ansvar

- Leder (avdelingsleder/seksjonsleder/enhetsleder) er ansvarlig for å gjøre prosedyre kjent blant ansatte og legge til rette for at prosedyren følges.
- Den enkelte ansatte har selv ansvar for å kjenne til og følge prosedyren.

## 3. Fremgangsmåte

I forkant av en videokonsultasjon må medisinskfaglig ansvarlig gjøre en vurdering om det er faglig forsvarlig å gjennomføre den polikliniske konsultasjonen som en videokonsultasjon. En slik måte å gjennomføre konsultasjonene på endrer ikke de ordinære ansvarsforhold. Den som yter helsehjelp har som alltid ansvar for at pasienten mottar nødvendig informasjon om sin helsetilstand og om hvordan helsehjelpen ytes. Det må som alltid også vurderes om man innehar relevant og nødvendig informasjon til å gjøre forsvarlige vurderinger i konsultasjonen, evt. om forsvarlig oppfølging fordrer personlig oppmøte m.m.

Følgende punkter bør være vurdert:

- Pasientens samtykke og personvern
- Pasientens forutsetninger
- Om formålet i konsultasjonen egner seg presentert og/eller er gjennomførbart via videokonsultasjon

Det anbefales at hver enkelt avdeling utarbeider egne retningslinjer/prosedyrer med klare føringer på når man skal/ikke skal benytte videokonsultasjon til avdelingens pasienter. Viser til prosedyren «Klinisk bruk av Confrere ved OUS» (eHåndbok id#136858).

### Samtykke og personvern

For at pasienten skal kunne samtykke til å motta helsehjelp via videokonsultasjon må det gis god informasjon om hva dette innebærer. Det er helsepersonell med faglig ansvar for helsehjelpen som skal gi denne informasjonen. Informasjonen som gis skal være tilpasset den enkelte pasient, og det skal så langt som mulig sikres at pasienten er klar over og forstår følgende informasjon:

- Bruk av videokonsultasjon er frivillig, og det er mulig å be om en oppmøtekonsultasjon istedenfor videokonsultasjon.
- Videokonsultasjonen er kryptert (sikkert) og det blir ikke gjort opptak av konsultasjonen.
- På samme måte som ved personlig oppmøte, vil helsepersonellovens regler om taushetsplikt være styrende for selve konsultasjonen og behandlingen av informasjon som fremkommer under samtalen.
- Relevant helseinformasjon blir journalført av helsepersonell på lik linje som om konsultasjonen skulle foregå som oppmøtekonsultasjon eller per telefon.
- Pasienten må sørge for å sitte/oppholde seg slik at samtalen ikke kan overhøres av andre som pasienten ikke ønsker å ha som tilhører.
- Pasienten avgir sitt samtykke til bruk av videokonsultasjon ved å akseptere invitasjonen til den enkelte videokonsultasjon.

### Forutsetninger for bruk av videokonsultasjon

Pasientens forutsetninger må vurderes før gjennomføring av en videokonsultasjon. Dette innebefatter:

- Pasientens teknologikompetanse
- Pasientens tilgang på utstyr
- Pasientens språklige barrierer
- Om pasienten har syn-/hørselshemming
- Eventuelle andre forhold som kan påvirke pasientens evne til å gjennomføre en videokonsultasjon

### Formålet med konsultasjonen

Ved følgende formål anbefales det ikke å benytte videokonsultasjon:

- Kliniske undersøkelser
- Stille diagnose
- Formidle alvorlig diagnose og negative beskjeder/resultater

## 4. Referanser

- Faktaark 54 – Videokonsultasjon – sjekkliste v1.0 (Direktoratet for eHelse)
- Normen v6.0 (Direktoratet for eHelse)
- Video – lyd og bildeopptak i helse og omsorgssektoren v1.0
- https://ehelse.no/aktuelt/korona-kom-i-gang-med-videokonsultasjon

**Andre eHåndboksdokumenter**

- Forvaltning av Confrere i OUS
- Klinisk bruk av Confrere ved OUS
- Pasientinformasjon - bruk av Confrere (OUS)

## Bakgrunn for kartleggingen

I takt med digitaliseringen av helsevesenet øker også avhengighetene mellom IKT, pasientbehandling og pasientsikkerhet. Forsvarlig helsehjelp skal være ivaretatt også når IKT-systemene er utilgjengelige.

Formålet med kartleggingen er å bidra til å sikre at forsvarlig helsehjelp også kan ytes ved bortfall av IKT. I denne kartlegging undersøker vi hvordan virksomhetene er forberedt på å håndtere situasjoner hvor kritiske IKT-system ikke er tilgjengelig. Dere blir blant annet bedt om å sende informasjon om virksomhetens rutiner for risikovurderinger på IKT-området, noen gjeldende risiko- og sårbarhetsanalyser for bortfall av IKT-systemer, noen nødrutiner for å håndtere bortfall av IKT-systemer, rutine for å oppdatere planene, gjøre de kjent og implementert i virksomheten. Herunder har vi også noen generelle spørsmål vedrørende bruk av avviksrapporter og risikovurderinger innen IKT-arbeidet.

Basert på funnene fra kartleggingen kan det bli aktuelt å vurdere andre former for tilsynsaktiviteter på et senere tidspunkt. Ved innsending av dokumenter ber vi om at dere bruker relevant spørsmålsnummer i begynnelsen av filnavn for dokumentet.

## Basisopplysninger

1. Navn på virksomheten

2. Hvem har besvart undersøkelsen?

3. Rolle og tittel for den som har svart

## Risikovurderinger

Nødrutiner og beredskapsplaner må bygge på risikovurderinger for de mest kritiske systemene. Vi forutsetter at dere samarbeider med relevant IKT-driftsleverandør ved innsending av svar der oppgaveutførelse er delegert.

4. Blir det gjort risikovurderinger ved alle IKT-endringene som kan ha store konsekvenser forvirksomheten?
   - Ja, send oversikt over alle kjente IKT-endringer utført 2020 med mulige konsekvenser for kliniske applikasjoner (endringer innen sentral infrastruktur etc.), kopi av første risikovurdering ved endring infrastruktur og første risikovurdering ved oppgradering et klinisk system utført 2020. Husk å bruke spørsmålsnummer (4) i begynnelsen av filnavn.
   - Delvis/vet ikke. Send oversikt over alle kjente IKT-endringer utført 2020 med mulige konsekvenser for kliniske applikasjoner (endringer innen sentral infrastruktur etc.), kopi av første risikovurdering ved endring infrastruktur, og første risikovurdering applikasjonsoppgradering utført 2020. Husk å bruke spørsmålsnummer (4) i begynnelsen av filnavn.
   - Nei, vennligst send inn oversikt over alle IKT-endringer utført 2020.

5. Hvilke tema er vurdert i risikovurderingen som er innsendt vedrørende endring av infrastruktur (forrige spørsmål)? (Flere svaralternativ)
   - Konfidensialitet
   - Tilgjengelighet
   - Dataintegritet
   - Forsvarlige helsetjenester
   - Ressursbruk helsepersonell som følge av endring i arbeidsprosesser
   - Ressursbruk IKT-personell som følge av endring i arbeidsprosesser
   - Annet (vennligst spesifiser)

6. Hvilke tema er vurdert i risikovurdering som er innsendt vedrørende oppgradering av klinisk system (spørsmål 4)? (Flere svaralternativ)
   - Konfidensialitet

- Tilgjengelighet
- Dataintegritet
- Forsvarlige helsetjenester
- Ressursbruk helsepersonell som følge av endring i arbeidsprosesser
- Ressursbruk IKT-personell som følge av endring i arbeidsprosesser
- Annet (vennligst spesifiser)

## ROS

**7.** Hvem utfører risikovurderinger ved IKT-endringer som kan ha konsekvenser for virksomheten? (Flere svaralternativ)

- Vi gjør egne risikovurderinger
- Vi gjør risikovurderinger sammen med IKT-driftsleverandøren
- IKT-driftsleverandøren gjør dette
- Varierende, ut fra situasjonen
- Det gjøres endringer uten kjent risiko
- Annet (vennligst spesifiser)

**8.** Hvilke tema blir vanligvis risikovurdert ved endring av kliniske applikasjoner (eks. EPJ-oppgradering)? (Flere svaralternativ)

- Konfidensialitet
- Tilgjengelighet
- Dataintegritet
- Forsvarlig helsetjeneste
- Ressursbruk helsepersonell som følge av endring i arbeidsprosesser
- Ressursbruk IKT-personell som følge av endring i arbeidsprosesser
- Annet (vennligst spesifiser)

**9.** Hvilke tema blir vanligvis risikovurdert ved endringer i IKT-infrastruktur? (Flere svaralternativ)

- Konfidensialitet
- Tilgjengelighet
- Dataintegritet
- Forsvarlig helsetjeneste
- Ressursbruk helsepersonell som følge av endring i arbeidsprosesser
- Ressursbruk IKT-personell som følge av endring i arbeidsprosesser
- Annet (vennligst spesifiser)

## Usikkerhet, e-konsultasjon

**10.** Blir usikkerhet i ulike typer risikovurderinger vurdert og dokumentert?

- Ja, omtrent alltid
- Ofte
- Noen ganger
- Nei, svært sjelden
- Annet (vennligst spesifiser)

## E-konsultasjoner (telefon, video, e-meldinger)

**11.** Er det gjort risikovurderinger av bruk av e-konsultasjoner (video, telefon, e-meldinger) opp mot fysiske pasientmøter, og hvilke tema er i så fall vurdert? Send inn ev. overordnet risikovurdering. Husk å bruke spørsmålsnummer (11) i begynnelsen av filnavn. (Flere svaralternativ)

- Ikke gjort risikovurdering med fokus på forsvarlig helsehjelp
- Utilstrekkelig undersøkelse/anamnese og forsinket helsehjelp
- Utilstrekkelig undersøkelse/anamnese og feil behandling
- Uoversiktlig og feil legemiddelbehandling
- Fordeler med tanke på smittereduksjon, ønske fra pasient i psykiatri eller andre fordeler
- Annet (vennligst spesifiser)

**12.** Er det registrert avvik knyttet til e-konsultasjoner (video, telefon, e-meldinger) siste halvår?
- Ja. Send oversikt. Husk å bruke spørsmålsnummer i begynnelsen av filnavn.
- Nei
- Annet (vennligst spesifiser)

## Kritiske system

Kritiske system inneholder ofte kliniske opplysninger som er nødvendige for å gi forsvarlig helsehjelp.

**13.** Er det identifisert hvilke systemer som er mest kritiske og der bortfall kan ha direkte konsekvenser for forsvarlig helsehjelp?
- Ja. Vennligst send inn en liste over disse. Husk å bruke spørsmålsnummer (12) i begynnelsen av filnavn.
- Nei
- Delvis. Vennligst send inn en liste over disse. Husk å bruke spørsmålsnummer (12) i begynnelsen av filnavn.

**14.** Hvem godkjente listen?
- Administrerende direktør
- Fagdirektør/medisinsk direktør
- Linjeleder klinisk avdeling
- IKT-leder / leder e-helse
- Andre. Vennligst spesifiser

**15.** Hvilke IKT-system drifter virksomheten ev. selv? (Flere svaralternativ)
- Sykesignalsystem
- Telefonisystem
- Stansalarmer
- Annet (vennligst spesifiser)

## Totalt bortfall av IKT

Følgende spørsmål gjelder bortfall av all IKT. Det vil for eksempel si bortfall av IKTsystem/ applikasjoner, fast- og trådløse nettverk, fasttelefon/IP-telefon, mobiltelefoner, overfallsalarmer, sykesignalanlegg, callinger.

**16.** Er en situasjon med bortfall av all IKT risikovurdert?
- Ja, send inn. Husk å bruke spørsmålsnummer i begynnelsen av filnavn.
- Nei
- Delvis, send inn. Husk å bruke spørsmålsnummer i begynnelsen av filnavn.

**17.** Er det laget en egen nødrutine for bortfall av all IKT?
- Ja. Vennligst send den inn. Husk å bruke spørsmålsnummer i begynnelsen av filnavn.

- Nei
- Delvis. Vennligst send inn det som finnes. Husk å bruke spørsmålsnummer i begynnelsen av filnavn.

**18.** Er nødrutinen for bortfall av all IKT testet i øvelser for personell?

- Testet i reell drift
- Ja, vi har hatt øvelse
- Nei, ikke gjort øvelse
- Annet (vennligst spesifiser)

## Planlegging av beredskap

Den som har det overordnede ansvaret for virksomheten skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter. Virksomhetens aktiviteter skal planlegges, gjennomføres, evalueres og korrigeres i samsvar med krav fastsatt i eller i medhold av helse- og omsorgslovgivningen.

Helseforetak har ansvar for å levere forsvarlige helsetjenester uansett om IKT-tjenester faller bort, og må derfor implementere forsvarlige nødrutiner for kritiske IKT-system.Tydelig oppgavefordeling og rolleavklaring mellom IKT-driftsleverandør og virksomhetene er viktig for styring av IKT.

**19.** Har virksomheten oversikter over avvik i pasientbehandling som er forårsaket av IKT-problemstillinger (eksempelvis bortfall, feil)?

- Ja. Vennligst send inn oversikter som viser årsak og konsekvenser. (Husk å bruke spørsmålsnummer i begynnelsen av filnavn.)
- Delvis. Vennligst send inn oversikter som viser årsak og konsekvenser. (Husk å bruke spørsmålsnummer i begynnelsen av filnavn.)
- Nei
- Annet (vennligst spesifiser)

**20.** Følger helseforetaket opp at IKT-feil som er meldt til IKT-driftsleverandør sitt kundesenteret blir fulgt opp ihht risiko knyttet til pasientsikkerhet?

- Vi (helseforetaket) følger opp at alle feil knyttet til pasientsikkerhet blir rettet av IKT-driftsleverandør
- Det varierer om vi (helseforetaket) følger opp at feil/endringsønsker blir rettet av IKT-driftsleverandør
- Vi (helseforetaket) følger sjelden opp feilretting av enkeltsaker meldt til IKT-driftsleverandør
- Ingen saker blir fulgt opp fra helseforetaket
- Annet (vennligst spesifiser)

**21.** Blir IKT-feil som er meldt til IKT-driftsleverandør sitt kundesenteret kategorisert, prioritert og fulgt opp ihht risiko knyttet til pasientsikkerhet? Send inn oversikt over de fem mest risikofylte feil/endringsønsker som IKT-driftsleverandør har registrert, dato for innrapportering og relevante pågående/planlagte tidfestede tiltak. (Husk å bruke spørsmålsnummer i begynnelsen av filnavn.)

- Ja, alltid
- Ofte
- Kun feil (ikke endringsønsker)
- Nei
- Vet ikke
- Annet (vennligst spesifiser)

**22.** Sikrer helseforetaket at IKT-driftsleverandør får informasjon om IKT-relaterte avvikssaker i helsetjenesten (som er meldt i virksomheten sitt avvikssystem)? (Flere svaralternativ)

- Ja, vi oversender/melder alle saker
- Delvis, vi oversender alle kjente saker i foretaksledelsen
- Delvis, avhengig av at helsepersonell melder saker
- Nei, vi oversender ikke IKT-relaterte avvikssaker
- Annet (vennligst spesifiser)

## Avvik

**23.** Hvem holder samlet oversikt over IKT-relaterte avvikssaker knyttet til forsvarlig helsehjelp? (Flere svaralternativ)

- IKT-driftsleverandør
- Helseforetaket
- Ingen
- Annet (vennligst spesifiser)

**24.** Hvem sikrer oppfølging av de viktigste sakene som har betydning for forsvarlig helsehjelp?

- Helseforetaket
- IKT-leverandøren
- Ingen
- Annet (vennligst spesifiser)

**25.** Hvordan følges ev. IKT-relaterte saker som er meldt inn i virksomheten sitt avvikssystem opp? Beskriv kort.

## Nødrutiner

**26.** Hvordan lagres nødrutiner for å sikre at de er tilgjengelige også ved bortfall * av nettverk?(Flere svaralternativer)

- På papir i beredskapspermer på alle kliniske avdelinger
- På papir i beredskapspermer ved noen kliniske avdelinger
- Lokale disker på alle kliniske avdelinger
- Lokale disker ved noen kliniske avdelinger
- Annet (vennligst spesifiser)

**27.** Sørger helseforetaket for jevnlig forbedring/oppdatering av nødrutiner?

- Ja, nødrutiner oppdateres jevnlig ved alle øvelser og store oppgraderinger av kliniske system.
- Vi har ikke strukturert oppdatering av nødrutiner for IKT-system etter øvelser eller store oppgraderinger av kliniske system.
- Annet (vennligst spesifiser)

**28.** Hvordan blir nødrutiner gjort kjent for nyansatte i organisasjonen? (Flere svaralternativ)

- Alle nyansatte sykepleiere og leger får informasjon i en form for kurs eller opplæring fra egen leder.
- Noen nyansatte sykepleiere og leger får informasjon i en form for kurs eller opplæring fra egen leder.
- Få nyansatte sykepleiere og leger får informasjon i en form for kurs eller opplæring fra egen leder.
- Det er betydelige variasjoner i hvor mye relevant opplæring leger og sykepleiere får.
- Annet (vennligst spesifiser)

**29.** Hvordan blir nødrutiner kontinuerlig opplyst om i organisasjonen for å vedlikeholde kompetanse hos ansatte? (Flere svaralternativ)

›

- Alltid informasjon til ansatte ved vesentlige oppdateringer
- Ofte informasjon til ansatte ved vesentlige opppdateringer
- Kurs sikrer vedlikehold av kompetanse
- Jevnlige øvelser
- Det er betydelige variasjoner i hvor mye relevant opplæring leger og sykepleiere får
- Annet (vennligst spesifiser)

## AMK

**30.** Har virksomheten egen AMK-sentral?

- Ja
- Nei

**31.** Når ble personell sist øvd i bruk av nødrutinen for bortfall av medisinsk nødtelefon (113)? (Skriv 1.1.2000 dersom personell ikke har øvd bruk av nødrutinen.)

Dato MM/DD/ÅÅÅÅ

**32.** Hvordan sikres innbyggerne forsvarlig helsehjelp hvis AMK-sentralen mister tilgang til 113 og sentrale IKT-system?

- Avtale med annen AMK i regionen
- Avtale med en AMK-sentral i en annen region
- Avtale både med AMK-sentral i egen region og i en annen region
- Annet (vennligst spesifiser)

**33.** Er risikoen for at den andre AMK-sentralen som skal overta ved feil, også kan være rammet av det samme problemet? Skriv kort hvilke vurderinger som er gjort.

## Akuttmedisinsk Informasjonssystem (AMIS) og Transmed

**34.** Når ble personell sist øvd i bruk av nødrutinen for Amis? (Skriv 1.1.2000 dersom personell ikke har øvd bruk av nødrutinen.)

Dato MM/DD/ÅÅÅÅ

**35.** Når ble personell sist øvd i bruk av nødrutinen for Transmed? (Skriv 1.1.2000 dersom personell ikke har øvd bruk av nødrutinen.)

Dato MM/DD/ÅÅÅÅ

## EPJ forsvarlighet

**36.** Fører bortfall av EPJ og røntgensystem til utsettelse av operasjoner?

- Ja, alle operasjoner stanses uansett hastegrad
- Mange operasjoner utsettes, også operasjoner som er nødvendig for å gi forsvarlig helsehjelp
- Noen operasjoner stanses midlertidig, alle operasjoner som er nødvendig for å gi forsvarlig helsehjelp utføres
- Få/ingen operasjoner påvirkes av IKT-bortfall
- Annet (vennligst spesifiser)

**37.** Hvor lenge vurderer dere at tilgang til å lese DIPS/DocuLive kan være borte før det blir vesentlig risiko for svikt i noen (forsvarlige) helsetjenester?

- Mindre enn 1 time
- 1 time
- 2 timer
- 3 timer

- 6 timer
- Annet (vennligst spesifiser)

**38.** Hvem har gjort sist nevnte vurdering over (fagbakgrunn og rolle)? (Fritekst)

## EPJ lesekopier

Selv om journalsystemet ikke er tilgjengelig for vanlig bruk kan en sette opp ulike alternativer. Med EPJ lesekopi menes her en kopi av journalsystemet som helsepersonell kan bruke for å lese journaldata, men som det ikke kan skrives i.

**39.** Hvilken informasjon og beslutningsstruktur gjelder vedrørende etablering av lesekopi av EPJ som tiltak ved ulike typer IKT-endringer?(Flere svaralternativ)

- Beslutning om å etablere lesekopi gjøres hos IKT-driftsleverandør etter delegert ansvar med avklarte kriterier. Send inn kriterier (husk spørsmålsnummer i filnavn).
- Helseforetaket blir informert om all risikofylte endringer og kan vurdere/bestille oppsett av lesekopi ved behov.
- Helseforetaket har fullgode nødrapporter fra EPJ for alle inneliggende og andre pasienter som kan trenge akutt hjelp, og trenger ikke lesekopi av EPJ for å sikre forsvarlig helsehjelp.
- Regional fagdirektør avgjør når det skal etableres lesekopi av EPJ.
- Helseforetaket mangler informasjon og/eller beslutningsstruktur er uklar.
- Annet (vennligst spesifiser)

**40.** Blir det gjort oppslag i kritisk informasjon i Kjernejournal ved EPJ-nedetid? Send inn rutiner for oppslag og registrering av kritisk informasjon (i Kjernejournal og interne system). Husk spørsmålsnummer i filnavn.

- Ja, ofte
- Noen ganger
- Sjelden
- Annet (vennligst spesifiser)

**41.** Hvordan kan helsearbeidere lese journaldata ved ulike typer IKT-feil? Sett kryss ved muligheter som er etablert eller beskriv løsning. (Flere svaralternativ)

- Etablert permanent oppdatert sentral lesekopi og nødrutine for å kunne lese i EPJ ved IKT-feil
- Etablert permanent oppdatert lokal lesekopi og nødrutine for å kunne lese i EPJ ved IKT-feil
- Tilstrekkelig journalinformasjon er lagret som kritisk informasjon i Kjernejournal, og Kjernejournal er tilgjengelig via mobilnett
- Nødrutine for utskrifter/rapporter fra EPJ ved driftsstans som sikrer tilgang til journalopplysninger (kun for innlagte pasienter)
- Annet (vennligst spesifiser)

## EPJ nødrutine

**42.** Finnes en overordnet nødrutine for bruk ved bortfall av DIPS/DocuLive?

- Ja. Vennligst send den inn. (Husk å bruke spørsmålsnummer i begynnelsen av filnavn.)
- Nei

**43.** Sørger nødrutiner for sikker og effektiv bestilling/svar på blodprøver og røntgen når IKT-løsningene ikke fungerer?

- Ja, vennligst send inn dersom den ikke inngår i allerede innsendt materiale (forrige spørsmål)

- Delvis, vennligst send inn dersom den ikke inngår i allerede innsendt materiale (forrige spørsmål)
- Har ikke nødrutiner for bestilling/svar laboratorie- og røntgenundersøkelser
- Annet (vennligst spesifiser)

**44.** Sørger nødrutiner for at det finnes en kontinuerlig oppdatert oversikt over inneliggende pasienter ved bortfall av det pasientadministrative systemet?
- Ja, vennligst send inn dersom den ikke inngår i allerede innsendt materiale
- Delvis, vennligst send inn dersom den ikke inngår i allerede innsendt materiale
- Nei
- Annet (vennligst spesifiser)

**45.** Sørger nødrutiner for at det finnes en kontinuerlig oppdatert oversikt over planlagte pasienter ved bortfall av det pasientadministrative systemet?
- Ja, vennligst send inn dersom den ikke inngår i allerede innsendte materiale
- Delvis, vennligst send inn dersom den ikke inngår i allerede innsendte materiale
- Nei
- Annet (vennligst spesifiser)

**46.** Når ble personell sist øvd i bruk av nødrutinen for DIPS/DocuLive? (Skriv 1.1.2000 dersom personell ikke har øvd bruk av nødrutinen.)

Dato DD/MM/ÅÅÅÅ

## EPJ risikovurdering

**47.** Når ble DIPS/DocuLive sist oppgradert? Send inn risikovurdering for siste oppgradering som er gjort av DIPS/DocuLive. Husk å bruke spørsmålsnummer i begynnelsen av filnavn. (Se bort fra ønske om innsendelse her dersom vurderingen er utført i 2020 og allerede sendt inn i forutgående spørsmål.)
- Utført 2020
- Utført 2019
- Utført 2018
- Annet (vennligst spesifiser)

**48.** Hvilken fagutdannelse/formal kompetanse har de som har vært med å lage risikovurderingen for oppgradering DIPS/DocuLive? (Flere svaralternativ)
- IKT
- Lege
- Sykepleier
- Helsesekretær
- Annet (vennligst spesifiser)

**49.** Hvordan var helseforetaket involvert i risikovurderingen for oppgradering av DIPS/DocuLive? (Flere svaralternativ)
- Deltok
- Fikk risikovurdering tilsendt til beslutning
- Fikk risikovurdering tilsendt til orientering
- Annet (vennligst spesifiser)

**50.** Hvem har godkjent restrisikoen for oppgradering av DIPS/DocuLive? (Flere svaralternativ)
- Adm.dir. i helseforetaket vårt
- Fagdirektør helseforetaket vårt

- Leder IKT-driftsselskap
- Regional fagdirektør
- Annet (vennligst spesifiser)

**51.** Hvilke tema er vurdert i risikovurderingen for DIPS/DocuLive? (Flere svaralternativ)
- Endring av alle funksjoner knyttet til forsvarlig helsehjelp
- Konfidensialitet
- Tilgjengelighet
- Dataintegritet
- Ressursbruk knyttet til endring av arbeidsprosesser
- Annet (vennligst spesifiser)

## EPJ oppetid

**52.** Hva sier IKT-driftsleverandør om estimert oppetid for EPJ? Angi i prosent. (Fritekst)

**53.** Hvilket tidsrom er denne oppetiden estimert og oppgitt for?
- Per uke
- Per måned
- Per år
- Vet ikke

**54.** Hvor mange minutter til sammen har EPJ vært opplevd som totalt utilgjengelig (uten lesekopi) av helsepersonellet ved akuttmottak i 2019? (Fritekst)

**55.** Hvor mange minutter til sammen har EPJ vært opplevd som tilgjengelig for lesing, men ikke tilgjengelig for skriving av helsepersonellet ved akuttmottak (dvs. bruk av lesekopi for EPJ) i 2019? (Fritekst)

**56.** Hva sier IKT-driftsleverandør om levert oppetid (i 2019) for EPJ? Angi i prosent. (Fritekst)

**57.** Er dette oppetid slik brukerne har opplevd den?
- Ja
- Nei, det er systemets oppetid (sentralt)
- Annet (vennligst spesifiser)

## Elektronisk kurveløsning

**58.** I hvilke enheter har virksomheten elektronisk kurveløsning? (Flere svaralterenativ)
- Psykiatriske sengeposter
- Somatiske sengeposter
- Akuttmottak
- Intensivenhet(er)
- Anestesi
- Annet (vennligst spesifiser)

**59.** Sikrer nødrutine for kurve sikker utdeling av legemiddel når elektronisk(e) kurveløsning(er) ikke fungerer?
- Ja
- Delvis
- Nei
- Ingen avdelinger bruker elektronisk kurve enda

- Annet (vennligst spesifiser)

**60.** I hvilke IKT-system finnes informasjon om legemiddelbehandling som pasienten mottar, og eventuelle legemiddelallergier? (Flere svaralternativ)
- Elektronisk kurve
- DIPS/DocuLive (skjema for kritisk informasjon)
- Separat operasjonsplanleggingssystem
- Reseptformidler
- Separat anestestesi-/intensivsystem
- Kjernejournal
- DIPS medikamentmodul
- Annet (vennligst spesifiser)

**61.** Er informasjon om legemiddelbehandling/-allergi automatisk synkronisert mellom system valgt over (oppgi ev. antall pålogginger)? (Fritekst)

## Røntgensystemet, RIS/PACS

**62.** Når ble personell sist øvd i bruk av nødrutinen for bortfall av røntgen-/multimediasystem? (Skriv 1.1.2000 dersom personell ikke har øvd bruk av nødrutinen.)

Dato DD/MM/ÅÅÅÅ

## Nødnett

**63.** Hvor brukes Nødnett i virksomheten? (Flere svaralternativ)
- AMK
- Ambulansene
- Akuttmottak
- Intern varsling
- Andre områder. Vennligst spesifiser

**64.** Har hvert bruksområde en nødrutine for bruk ved bortfall av systemet?
- Ja
- Nei
- Annet (vennligst spesifiser)

## Analogtelefon, IP-telefon eller DECT

**65.** Når ble helsepersonell sist øvd i nødrutine for de ulike telefoniløsningene? (Skriv 1.1.2000 dersom personell ikke har øvd bruk av nødrutinen.)

Dato MM/DD/ÅÅÅÅ

## Mobiltelefon

**66.** Når ble personell sist øvd i bruk av nødrutinen for mobilnettverk? (Skriv 1.1.2000 dersom personell ikke har øvd bruk av nødrutinen.)

Dato DD/MM/ÅÅÅÅ

**67.** Sikrer nødrutinen at bakvakter kan kalles inn, også når hovedleverandørens mobilnett * er ute av drift?
- Ja
- Delvis, men mye vanskeligere
- Nei
- Annet (vennligst spesifiser)

## Sykesignalanlegg og stansalarmer

**68.** Gi en kort beskrivelse av gjeldende nødrutine for bortfall av sykesignalanlegg. (Fritekst)

**69.** Når ble personell sist øvd i bruk av nødrutinen for bruk ved bortfall av stansalarmer? (Skriv 1.1.2000 dersom personell ikke har øvd bruk av nødrutinen.)

Dato DD/MM/ÅÅÅÅ

Siste side

**Takk for svar**

# 6

# Samisk og engelsk sammendrag

# Dohkálaš pasieantadikšu IKT haga?

RISKAÁRVVOŠTALLAMAT, HEAHTERUTIINNAT JA BUORIDANDOAIMMAT 17 BUOHCCIVIESUS
RAPORTA 2/2021
NJUKČAMÁNNU 2021

2020:s čađahii Stáhta dearvvašvuođageahčču kártema 17 Norgga buohcciviesu kritihkalaš vuogádagain, riskaárvvoštallamiin ja heahterutiinnain mat sis leat IKT-vuogádagaide. Gávdnosat kártemis čájehit ahte doaimmahagat leat ráhkadan máŋga riskaanalysa IKT-rievdamiidda. Muhto leat ráhkaduvvon unnán riskaárvvoštallamat mat muitalit mo lea jus IKT jávká oalát.

Eanaš riskaanalysain deattuhuvvojit teknihkalaš áššit, muhto unnán mo váikkuhivčče klinalaš doaimmaide jus IKT jávkkašii oalát. Dearvvašvuođadoaimmahagain váilo vuogádatlaš oppalašgeahčastat das guđemuš IKT-áššiin leat stuorámus váikkuhusat dearvvašvuođaveahkkái ja pasieantasihkarvuhtii. Lea maiddái eahpečielga ovddasvástádusjuohkin gaskal RHF, HF ja IKT-doaibmalágideaddji go dát áššit galget vuoruhuvvot.

Mađi guhkit IKT lea jávkan dađi stuorát riska ahte šaddet boasttuvuođat dearvvašvuođabálvalusain. Buohcciviesut masset johtilit oppalašgeahčastaga iežaset sisačálihuvvon pasieanttain. Fáhkkabuhcciid vuostáiváldimis leat ollu pasieanttat maid dilli ii leat čielggaduvvon, ja riska boasttudikšui stuorru go ii dovdda pasieantta buozalmasvuođahistorjjá. Doaimmahagain váilot buori muddui heahtečovdosat dasa mo fidne dieđuid ođđa pasieanttaid birra go dábálaš journálavuogádat ii leat olámuttos. Eanetlohku doaimmahagain árvvoštallet ahte šaddá stuorra riska ahte leat váilevašvuođat dearvvašvuođabálvalusain unnitgo 2 diimmu dan rájes go EPJ-vuogádat lea jávkan.

Dearvvašvuođadoaimmahagat barget vuogádatlaččat ráhkadit heahterutiinnaid ja fuolahit ahte dearvvašvuođabargit hárjehallet daid geavahit. Doaimmahagain leat dattege menddo heajos heahterutiinnat ja/dahje hárjehallandábit muhttin teknihkalaš gulahallančovdosiidda nu mo alárpmaide ja telefoni:i. Dát lea kritihkalaš go čovdosat eanet ahte eanet leat čadnon IKT-fierpmádagaide, ja seammás leat guovddážis máŋgga heahterutiinnain mat buohcciviesuin leat.

Kárten čájeha maid ahte leat váilevaš ovttastusat dehálaš dieđuin pasieantta dálkkasgeavaheami birra. Vaikke vel dovdat makkár hástalusat leat dálkkasdiehtojuohkimiin ja “Okta ášši - okta journála” lea višuvdnan de leat máŋga doaimmahaga ásahan ođđa vuogádagaid main leat duplikáhta dieđut, main gáibiduvvo liige sisaloggen ja liige ohcan dearvvašvuođabargiin. ●

# Appropriate patient treatment without ICT?

RISK ASSESSMENTS, EMERGENCY PROCEDURES AND IMPROVEMENT WORK AT 17 HOSPITALS.
REPORT 2/2021
APRIL 2021

During 2020, the Norwegian Board of Health Supervision conducted a survey of critical systems, risk assessments and emergency procedures linked to ICT systems at 17 Norwegian hospitals. The findings made in the survey indicate that the trusts have prepared many risk analyses concerning ICT changes. However, few overall risk assessments have been prepared concerning the loss of all ICT services.

Most risk analyses focus on technical aspects, but little on the consequences of ICT loss in clinical activity. The health trusts have no systematic overview of the ICT cases that have the greatest consequences for appropriate healthcare and patient safety. The delegation of responsibility between regional health authorities, health trusts and ICT service providers is also unclear as regards the prioritisation of such matters.

The risk of failure in the health services increases the longer the loss of ICT continues. Hospitals rapidly lose track of admitted patients. In accident and emergency departments, many patients have unresolved conditions, and the risk of incorrect treatment increases when the patient's medical history is unknown. The health trusts lack adequate emergency solutions for access to information concerning new patients when the normal patient record system is unavailable. Most health trusts believe there will be a significant risk of failure in health services once the electronic patient record system has been inaccessible for two hours.

The health trusts are working systematically to develop emergency procedures and ensure that healthcare professionals are drilled in their use. However, the trusts have inadequate emergency procedures and/or practice regimes for some technical communication solutions such as alarms and telephone systems. This is critical because the solutions are increasingly being based on ICT networks, yet they are pivotal to many emergency procedures at hospitals.

The survey also revealed a lack of consistency in important data concerning the patient's use of medication. Despite known challenges relating to drug information and the vision of "One Citizen - One Health Record", many health trusts have introduced new systems with duplicate data, requiring additional log-ins and patient lookups for healthcare professionals.

## Videre lesning på www.helsetilsynet.no

Om IKT-tilsyn på Helsetilsynets nettsider

Hvordan er sykehusene forberedt på IKT-bortfall. Kartlegging ved fem virksomheter. Rapport 3/2020

Helsetilsynets "IKT-tilsyn" - normen(e)s vokter og helsearbeidernes venn. Direktør Jan Fredrik Andresens innlegg på Normkonferansen 2019

Alle utgivelser i **Rapport fra Helsetilsynet** finnes i fulltekst med sammendrag på engelsk og samisk på www.helsetilsynet.no

ISBN 978-82-93595-41-0 Rapport fra Helsetilsynet 2/2021. **Forsvarlig pasientbehandling uten IKT? Risikovurderinger, nødrutiner og forbedringsarbeid ved 17 sykehus, elektronisk versjon**

# Forsvarlig pasientbehandling uten IKT?

# Risikovurderinger, nødrutiner og forbedringsarbeid ved 17 sykehus.

RAPPORT FRA HELSETILSYNET 2/2021 • APRIL 2021

Statens helsetilsyn gjennomførte i 2020 en kartlegging av kritiske system, risikovurderinger og nødrutiner for IKT-system ved 17 norske sykehus. Funn i kartleggingen viser at virksomhetene har utarbeidet mange risikoanalyser for IKT-endringer. Men det er utarbeidet få overordnede risikovurderinger for bortfall av all IKT.

De fleste risikoanalysene har fokus på tekniske forhold, men lite på konsekvenser av IKT-bortfall i klinisk virksomhet. Helseforetakene mangler systematisk oversikt over hvilke IKT-saker som har størst konsekvens for forsvarlig helsehjelp og pasientsikkerhet. Ansvarsfordelingen mellom RHF, HF og IKT-driftsleverandør er også uklar når det gjelder prioritering av slike saker.

Risikoen for svikt i helsetjenestene øker jo lenger IKT-bortfall varer. Sykehusene mister raskt oversikt over innlagte pasienter. I akuttmottakene har mange pasienter uavklarte tilstander, og risikoen for feilbehandling øker når man ikke kjenner pasientens sykehistorikk. Virksomhetene mangler i stor grad nødløsninger for tilgang til informasjon om nye pasienter når vanlig journalsystem er utilgjengelig. Flertallet av virksomhetene vurderer at det blir vesentlig risiko for svikt i helsetjenester etter mindre enn 2 timer når EPJ-system faller bort.

Helseforetakene arbeider systematisk med å utarbeide nødrutiner og sørger for at helsepersonellet øver på å bruke de. Virksomhetene har imidlertid for svake nødrutiner og/eller øvingsregimer for noen tekniske kommunikasjonsløsninger som alarmer og telefoni. Dette er kritisk fordi løsningene i stadig større grad baserer seg på IKT-nettverk, og samtidig er sentrale i mange nødrutiner ved sykehusene.

Kartleggingen avdekker også manglende konsistens i viktige data om pasientens legemiddelbruk. Til tross for kjente utfordringer med legemiddelinformasjon og visjon om «Én innbygger - én journal» har mange virksomheter innført nye system med duplikate data, krav til ekstra pålogging og ekstra oppslag (pasientsøk) for helsepersonell.

Helsetilsynet
TILSYN MED BARNEVERN, SOSIAL- OG HELSETJENESTENE

I serien Rapport fra Helsetilsynet formidles funn og erfaring fra klagebehandling og tilsyn med sosiale tjenester, barnevern- og helse- og omsorgstjenestene.

Serien utgis av Statens helsetilsyn. Alle utgivelser i serien finnes i fulltekst på www.helsetilsynet.no