Kartlegging ved fem virksomheter

Hvordan er sykehusene forberedt på IKT-bortfall?

Helsetilsynet
TILSYN MED BARNEVERN, SOSIAL- OG HELSETJENESTEN

RAPPORT 3/2020 • AUGUST 2020

Innhold

Innhold

Tabell- og figurregister

Tabellregister

Figurregister

1 Oppsummering

1.1 Om kartleggingen

Det er gjort en kartlegging av fem virksomheter sine oversikter over kritiske system, risikovurderinger og nødrutiner for IKT-system. Vi undersøkte i hvilken grad virksomhetene er forberedt på å håndtere situasjoner hvor sentrale kliniske IKT-system ikke er tilgjengelig. Herunder har vi sett på hvordan virksomhetene har vurdert risiko knyttet til å kunne yte forsvarlig helsehjelp ved bortfall av IKT, og hvordan de har laget planer og tiltak basert på risikovurderingene.

Det er ikke gjort en lovlighetskontroll av innsendte svar. Informasjonssikkerhet undersøkes for tilgjengelighet, men ikke for konfidensialitet eller integritet. Kvalitet i nødrutinene er ikke detaljert vurdert. Virksomhetene har gjort rede for testing, oppdatering, opplæring og publisering av nødrutiner. Kartleggingen er gjort ved hjelp av skriftlige og muntlige spørsmål, og dokumentinnsamling via kontaktpersoner ved sykehusene. Det er ikke undersøkt praksis ved kliniske avdelinger i virksomhetene.

1.2 Funn i kartleggingen

Det var en diskrepans mellom antall utførte endringer og innsendte risikovurderinger i kartleggingen. Vi ba om å få tilsendt de to siste risikovurderingene for endringer som kunne ha betydning for driften. Kartleggingsmetoden ga ikke oversikt over gjeldende praksis for risikovurderinger hos regionale IKT-driftsleverandører. Det var noe uavklart ansvar mellom noen helseforetak og IKT-driftsleverandører vedrørende utføring og godkjenning av risikovurderinger.

Virksomhetene har i stor grad identifisert hvilke IKT-system som er kritiske, og i stor grad utarbeidet nødrutiner for sentrale funksjoner i systemene. Oversiktene over kritiske IKT-løsninger har noen mangler. Hos noen virksomheter mangler tekniske løsninger som stansalarmer (akutt tilkalling av spesialister ved hjertestans eller lignende inne på sykehuset), sykesignalanlegg (signal fra pasient/'pasientsnor') og Nødnett i oversiktene. De har i varierende grad testet nødrutiner for disse tekniske løsningene. Nødrutinene er lagret slik at de er tilgjengelig for helsepersonell på kliniske avdelinger selv om IKT svikter. Det er noe varierende øving i nødrutiner, men i praksis får en test av nødrutiner ved reelle driftsproblem. Virksomhetene har i liten grad hentet ut rapporter fra avvikssystem for å se på konsekvenser og planlegge tiltak ved bortfall av IKT i helsetjenestene.

Kartleggingen viste at alle virksomhetene har nødrutiner for å ta blodprøver og bildeundersøkelser når EPJ-systemet er ute av drift. Det er imidlertid få virksomheter som klarer å holde oversikt over ›

inneliggende og planlagte pasienter ved IKT-bortfall. Fare for svikt i forsvarlige helsetjenester øker jo lengre periode IKT-feil varer. Pasienter som kommer til akuttmottaket mens journalsystem er utilgjengelig, må i stor grad behandles uten informasjon om tidligere behandling.

Virksomheter med utbredt bruk av elektronisk kurve har nødrutiner for forsvarlig legemiddelbehandling ved IKT-bortfall. Alle virksomhetene har nødrutiner for å føre journal for enkeltpasienter ved IKT-feil. Det er risiko for svikt i forsvarlig helsehjelp ved manglende lesetilgang i EPJ. Beslutningsstrukturer vedrørende etablering av lesekopier av EPJ (en elektronisk tilgang til å lese journal) er uklare ved flere virksomheter. Et tiltak som mange virksomheter trolig kan lære fra kartleggingen er etablering av en kontinuerlig oppdatert lesekopi av EPJ. Dersom EPJ (produksjonsdatabase) feiler vil da helsepersonell kunne lese pasientopplysninger i en kopi av EPJ. En region arbeider nå med å sette opp en lesekopi av EPJ som er kontinuerlig oppdatert. Dette fremstår som en god løsning for å sikre at journal alltid er tilgjengelig lokalt på sykehuset, og løsningen vil gi betydelig reduksjon av risiko.

Virksomhetene som deltok i kartleggingen ga tilbakemelding om at det var nyttig å svare på spørsmålene. Noen nødrutiner ble også testet i perioden.

Helsetilsynet opplevde at virksomhetene gjorde et grundig arbeid ved innsending av svar.

1.3 Videre arbeid

Det er viktig å avklare ansvarsforhold mellom virksomheter som har ansvar for leveranser av helsehjelp og IKT-driftsleverandørene de benytter. Et eksempel på område med behov for avklaring er utarbeiding av risikovurderinger og tiltak. Hvordan avviksrapporter benyttes i forbedringsarbeidet bør også undersøkes.

Tilgang til journalinformasjon må sikres for å tilby forsvarlig helsehjelp. Dette innebærer tilgang til viktig helseinformasjon, og oversikt over inneliggende og planlagte pasienter.

Kartleggingsspørsmål vil bli revidert og sendt ut til flere virksomheter.

2

Bakgrunn

«Forsvarlig helsehjelp vil i stadig større grad hvile på bruk av ulike tekniske løsninger.»

2.1 Lovgrunnlag

Helsetjenester som tilbys eller ytes skal være forsvarlige, jf. spesialisthelsetjenesteloven § 2-2. Forsvarlighetskravet er en rettslig standard, som er forankret i blant annet 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 pålagt å sikre forsvarlige tjenester gjennom sin styring. 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.

2.2 Utviklingstrender

I takt med digitaliseringen av helsevesenet øker avhengighetene mellom IKT, pasientbehandling og pasientsikkerhet. Det er i dag vanskelig å tenke seg forsvarlig drift av sykehus uten omfattende bruk av ulike IKT-system. Drift av IKT-løsninger blir samtidig sentralisert og gjort mer robust. Sentralisering kan utfordre styringsmodeller og ansvarsposisjoner, men samtidig effektiviseres IKT-driften. Oppetid og sikkerhet kan forbedres, men sentrale feil kan også få større konsekvenser ved at de slår ut system på flere sykehus samtidig.

Fremover forventer vi å se økt bruk av løsninger som elektronisk medikamentkurve, automatisk datafangst fra medisinsk teknisk utstyr, beslutningsstøtte og kunstig intelligens (1). Det er grunn til å anta at utvikling av IKT- og helsetjenester blir stadig mer integrert.

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

3 Besvarelser, metode og faktum

3.1 Antall besvarelser og metode

Kartleggingen er utført ved fem virksomheter i ulike helseregioner, og en av virksomhetene som inngikk i undersøkelsen er en privat ideell virksomhet. Det er et universitetssykehus blant respondentene. Det var tre virksomheter som hadde AMK-sentral, og det var tre virksomheter som hadde innført elektronisk kurve i hele eller deler av organisasjonen. Alle virksomhetene har besvart 79 spørsmål elektronisk.

Det er totalt sendt inn 135 dokumenter fra de ulike virksomhetene. Største del av de innsendte dokumentene er nødrutiner, og noen av dokumentene er oversikter over kritiske system, rapporter fra avvikssystem og risikovurderinger. Antall innsendte dokumenter fordelte seg slik:

Tabell 1 Antall dokumenter per virksomhet

	Virksomhet 1	Virksomhet 2	Virksomhet 3	Virksomhet 4	Virksomhet 5
Totalt antall dokumenter	68 (inkludert mange detaljer)	11	15	20	21

Kontaktpersonene som har besvart kartleggingen og sendt inn dokumenter har roller som leder for e-helse, IKT og/eller IKT-sikkerhet. Etter at vi hadde lest mottatte dokumenter hadde vi møter med hver kontaktperson for å sikre riktig forståelse av innsendte svar.

Vi ville undersøke i hvilken grad virksomhetene er forberedt på å håndtere situasjoner hvor sentrale kliniske IKT-system eller tekniske løsninger for stansalarm, Nødnett etc. ikke er tilgjengelig. Herunder ville vi se på hvordan virksomhetene har vurdert risiko knyttet til å kunne yte forsvarlig helsehjelp ved bortfall av IKT, og hvordan de har utviklet og implementert planer og tiltak basert på vurderingene.

Det er ikke gjort en lovlighetskontroll av innsendte svar. Informasjonssikkerhet undersøkes for tilgjengelighet, men ikke for konfidensialitet eller integritet. Kvalitet i nødrutinene er ikke detaljert vurdert.

Kartleggingen er avgrenset til noen virksomheter i spesialisthelse-tjenesten. Det er innhentet noen risikovurderinger fra virksomhetene. Basert på funnene fra kartleggingen kan det bli aktuelt å vurdere andre former for kartlegginger/tilsynsaktiviteter. Kartleggingen inkluderer ikke tiltak hos IKT-leverandører for å redusere risiko for IKT-bortfall.

Virksomhetene som deltok i kartleggingen ga tilbakemelding om at det var nyttig å svare på spørsmålene.

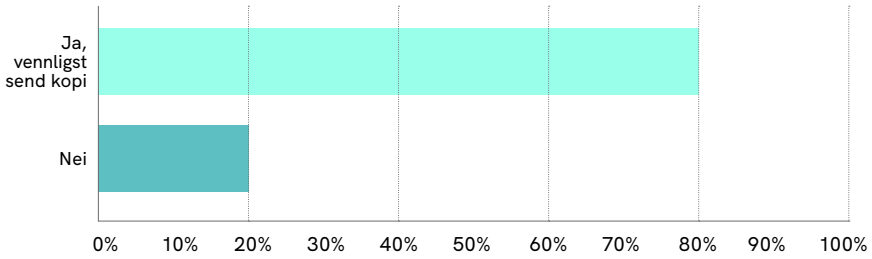
3.2 Hvilke IKT-system som er kritiske/viktigst for å kunne yte forsvarlig helsehjelp og sannsynligheten for at disse faller bort

3.2.1 Faktagrunnlag

3.2.1.1 Risikovurderinger

Fire av fem virksomheter svarte at det ble gjort risikovurderinger ved de to siste endringene på IKT-området som kunne ha store konsekvenser for virksomheten:

Figur 1 Andel foretak som har gjort risikovurderinger



Virksomhetene var bedt om å sende sine sist oppdaterte risiko-vurderinger som kan ha konsekvenser for virksomheten. Alder på de innsendte risikovurderingene var gjennomsnittlig ca. 1,5 år gamle. Det er gjort IKT-endringer (som oppgraderinger av applikasjoner og infrastruktur) som noen av sykehusene ikke har risikovurderinger av.

Det ble i spørsmål om hvem som utfører risikovurderinger ved IKT-endringer svart at alle gjør slike vurderinger selv, og fire virksomheter svarte at de også gjør vurderinger sammen med IKT-driftsleverandørene. I møte oppga virksomhetene at IKT-driftsleverandør ofte gjør risikovurderinger selv, og at alder på innsendte dokumenter derfor ikke var representativt for hyppighet av vurderinger som gjøres. De fleste virksomhetene har lite informasjon om risikovurderinger som IKT-driftsselskapene gjør. En virksomhet oppgir at de får alle planlagte IKT-endringer til vurdering via endringsråd (ITIL Change advisory board). Andre virksomheter får risikovurderinger for spesifikke IKT-system fra IKT-driftsleverandør til godkjenning hos relevant systemeier i virksomheten. Hos noen forutsettes det at systemeier i virksomheten holder rede på restrisiko, risikoreduserende tiltak og risiko i arbeidsrutiner. Det er ikke undersøkt ›

forutsetninger (eksempelvis myndighet og kompetanse) slike systemeiere har i virksomhetene.

For en del nye regionale system er representanter fra virksomhetene med og lager regionale risikovurderinger. Helsetilsynet spurte ikke om de enkeltes roller, kompetanse eller myndighet i disse risikovurderingene.

Ut fra innhold i tilsendte risikovurderinger og samtaler med kontakt-personer fremstår IKT-sikkerhet som hovedfokus i risikovurderinger som blir utarbeidet. Innenfor IKT-sikkerhet varierer det noe, samlet sett fokuseres det mest på personvern. Tre virksomheter har sendt inn risikovurderinger vedrørende videokonsultasjonsløsninger. Øvrige vurderinger varierte fra oppgradering/leveranser DIPS Arena til mindre forsknings- og laboratoriesystem. Ut fra innsendte risikovurderinger er det lite fokus på helsearbeiderens arbeidssituasjon og endringene i arbeidsprosessene etter IKT-oppdateringer. I mange av risiko-vurderingene er det uklart om helsepersonell har deltatt i vurderinger om konsekvenser/endringer i forhold til forsvarlig helsehjelp.

Ved noen virksomheter er det utydelig hvem som har ansvar for utarbeiding og godkjenning av risikoanalyser. Det er oppgitt en tydeligere ansvarsavklaring ved virksomheter der det benyttes en ekstern leverandør (sammenlignet med de som har interne og regionale driftsleverandører). Det ble ikke spurt om grad av usikkerhet, og ingen har heller oppgitt grad av usikkerhet i de innsendte risikovurderingene.

IKT-driftsleverandører sine rutiner for ROS og tiltak for risikoreduksjon er ikke undersøkt.

3.2.1.2 Identifisering av kritiske system

Oversikt over kritiske system er viktig grunnlag for å gjøre risikovurderinger, planlegge drift, tiltak ved IKT-bortfall og forebygging. Fire av fem virksomheter oppga at de hadde identifisert hvilke system som er mest kritiske og der bortfall kan ha direkte konsekvenser for forsvarlig helsehjelp. En virksomhet svarte at disse systemene var delvis identifisert.

Alle virksomhetene har sendt inn lister over kritiske system. Gjennomgang av innsendt dokumentasjon viste at to av fem virksomheter ikke hadde tatt med teknologi som sykesignalsystem, stansalarmer, mobiltelefoner og Nødnett i sine lister over kritiske system. For disse to inneholdt listen bare system som driftes av den regionale IKT-leverandøren og ikke systemene de drifter selv. Det er for øvrig stort samsvar mellom lister over kritiske applikasjoner ved de ulike virksomhetene.

«Det ble stilt spørsmål om en tenkt situasjon med bortfall av all IKT er risikovurdert.»

Alle virksomhetene svarte at administrerende direktør (eller ledergruppen) har godkjent listen.

Personell som hadde deltatt i utarbeiding av lister med kritisk system ble oppgitt til å ha varierende kompetanse. Alle virksomheter hadde personell med IKT-sikkerhetskompetanse i arbeidet. Fire av fem virksomheter hadde med lege og IKT-systemkompetanse i vurderingene. Tre av fem virksomheter hadde med sykepleiere og personell med kompetanse på IKT-infrastruktur, foruten at noen representanter i vurderingene ble oppgitt til å ha «annen» kompetanse.

3.2.1.3 Bortfall av alle IKT-baserte løsninger

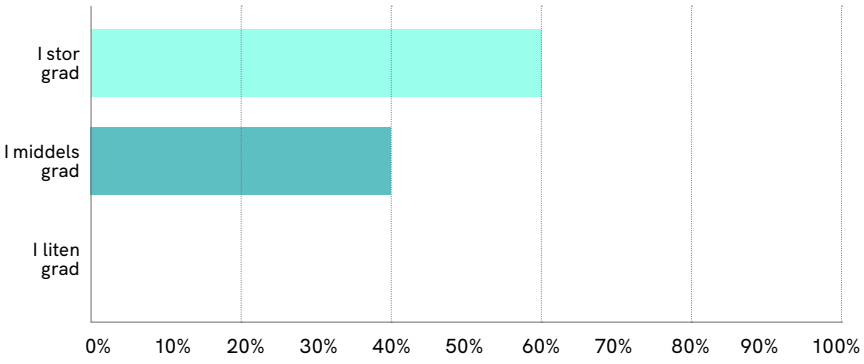
Det ble stilt spørsmål om en tenkt situasjon med bortfall av all IKT er risikovurdert. To virksomheter svarte at det var gjort, to virksomheter svarte at det var delvis gjort og en virksomhet svarte at dette ikke var gjort.

Tre virksomheter sendte inn en egen nødrutine for bortfall av IKT-nettverk og alle system. En virksomhet oppga at de delvis har laget en slik nødrutine. En virksomhet oppga at de ikke har laget egen nødrutine for bortfall av all IKT, men at de i praksis har nødrutiner dersom alt feiler.

På spørsmål om nødrutiner reduserer fare for svikt i helsetjenestene svarer virksomhetene slik:

Figur 2 Reduksjon av risiko

I hvilken grad vurderer virksomheten at nødrutinen reduserer faren for svikt i helsetjenesten?



Tre virksomheter oppgir at de har testet nødrutinen for bortfall av nettverk i reell drift. To virksomheter har testet rutine 'teoretisk' blant annet ved å gå gjennom scenarier i møte i beredskapsledelse.

3.2.1.4 Estimert oppetid for ulike IKT-løsninger

Virksomhetene som har deltatt i kartleggingen kjøper alle de fleste IKT-tjenestene fra IKT-driftsleverandører. Det varierer hvilke av de under nevnte tjenestene de kjøper, hvilke avtaler som er etablert for oppetid (tid system er tilgjengelig), hvordan de oppgir og måler oppetid.

Amis, akuttmedisinsk informasjonssystem

For funksjonell beskrivelse av Amis, se kap. 3.3.2. Oppetid som IKT-driftsselskapene har oppgitt til virksomhetene vedrørende systemet Amis er 98,5–99,99 prosent.

To av tre svarer at oppgitte tall er brukerne sin opplevelse av systemet sin oppetid. En virksomhet har svart at dette er selve systemet sin oppetid på server og inkluderer altså ikke nettverks- og klientfeil.

Transmed, styring av ambulansene

For funksjonell beskrivelse av Transmed se kap. 3.3.3. En virksomhet svarer at oppetid som et IKT-driftsselskap har oppgitt vedrørende systemet Transmed er 99,6 prosent. Virksomheten svarer at dette tilsvarer oppetid som brukerne opplever. En virksomhet har ikke fått oppgitt oppetid fra IKT-driftsselskap. Det tredje virksomheten med AMK-sentral svarer at selve systemet sin oppetid er oppgitt til 99,999 prosent. Dette er ikke oppetid slik brukerne vil oppleve den, men selve systemets oppetid på server.

Nødnett

Det er bare en virksomhet som har svart på spørsmål om HDO (Helsetjenestens Driftsorganisasjon) sine leveranser. De svarer at HDO leverer 99,95 prosent oppetid på Nødnett.

EPJ (elektronisk pasientjournal)

EPJ brukes her av praktiske årsaker om systemene DIPS og DocuLive EPR (øvrige kliniske system inneholder også journalinformasjon). Virksomhetene oppga at de har fått oppgitt følgende oppetid (prosent) for EPJ av sine IKT-selskap:

Tabell 2 Oppgitt oppetid

Oppgitt oppetid EPJ
99,997
99,7
99,6
100,0
99,97

To sykehus svarte at dette er oppetid slik brukerne vil oppleve den. Tre av virksomhetene svarte at dette er selve systemet sin oppetid (på server), og at denne oppetiden er ulik den oppetiden brukerne opplever.

Røntgensystem
Virksomhetene svarer at de har omtrent samme oppetid for røntgensystem som EPJ (forrige spørsmål), det vil her si mellom 99,7 og 100 prosent.

To virksomheter svarte at dette er oppetid slik brukerne opplever den. Tre virksomheter svarte at det er selve systemets oppetid.

Medikamentkurve
De regionale IKT-driftsselskapene har oppgitt 99,977 prosent som levert «oppetid på selve systemet» til en virksomhet og 100 prosent oppetid slik brukerne vil oppleve den til en annen virksomhet. Vi mangler data om oppetid for den tredje virksomheten med elektronisk kurve.

Analogtelefon, IP-telefon eller DECT (Digital Enhanced Cordless Telecommunication)
Virksomhetene oppgir 99,5–100 prosent oppetid for telefoniløsninger (en oppgir ukjent oppetid).

Sykesignalanlegg
Oppetid for sykesignalløsninger og stansalarmer er oppgitt til 99,5–99,99 prosent og ukjent ved en virksomhet.

Overfallsalarmer
Det er oppgitt oppetider for overfallsalarmer mellom 99,5–99,9 prosent og en ukjent.

3.2.2 Refleksjoner, vurderinger av funn

To av fem virksomheter hadde ikke tatt med teknologi som sykesignal-system, stansalarmer, mobiltelefoner og Nødnett i sine lister over kritiske system. Det kan for eksempel være fordi det har vært en gradvis overføring av slike tekniske løsninger til nettverk/IKT-baserte system, eller fordi en del sykehus selv alltid har hatt ansvar for slike system og at løsningene derfor ikke er inne på etablerte regionale lister hos IKT-driftsleverandører. Medisinsk utstyr og systemløsninger knyttet til MTU (medisinsk teknisk utstyr) er ikke vurdert i kartleggingen.

Det er innhentet noen risikovurderinger fra virksomhetene. Risiko-vurderingene virker til å være preget av at IKT-sikkerhet de siste årene har dreid seg mer om konfidensialitet enn IKT-bortfall og integritet. Det var en diskrepans mellom frekvens på endringer og innsendte risiko-vurderinger i kartleggingen. Kartleggingen gir ikke et tilstrekkelig bilde av gjeldende praksis for risikovurderinger. Helsetilsynet har heller ikke undersøkt IKT-driftsleverandører sine rutiner for utarbeiding av risikovurderinger. Ut fra svarene gitt i undersøkelsen og konklusjoner i tidligere tilsynssaker vedrørende IKT-sikkerhet (2), kan det virke som det er behov for å arbeide mer med denne ansvarsavklaringen ved flere ›

> «...ingen har oppgitt grad av usikkerhet i de innsendte risikovurderingene...»

helseforetak med regionale IKT-driftsleverandører. Det er ikke vurdert om oppetid er forskjellig ved bruk av ekstern leverandør, regional- eller intern MTA/IKT-avdeling.

Det kan virke som det er flest med IKT-kompetanse som er med og utarbeider IKT-risikovurderinger, og at det derfor blir mindre fokus på helsepersonellet sine muligheter til å gi forsvarlige helsetjenester. Det er en svakhet i metoden at det i kartleggingen ikke er spurt om helsepersonell med systemoversikt har deltatt i risikovurderinger. Det er heller ikke spurt om usikkerhet i risikovurderinger er vurdert.

Det er en svakhet i svarene at ingen har oppgitt grad av usikkerhet i de innsendte risikovurderingene, og vi vet ikke om dette skyldes manglende bevissthet eller dokumentasjon. Sannsynligvis mangler lederne som godkjenner risikovurderinger da også informasjon om usikkerhet i IKT-risikovurderinger. Virksomheter som benytter regionale IKT-driftsleverandører kan ha mindre myndighet over løsningene de benytter. Robusthet i løsningene og styringsmodeller er ikke nærmere undersøkt.

Erfaringer tilsier at IKT-endringer (oppdateringer) noen ganger har overraskende konsekvens for andre funksjoner, for eksempel i forbindelse med integrasjoner. Gode rutiner for testing er viktig, og gode rutiner for risikovurderinger er en forutsetning for å lage gode testscenarioer.

Det at eksisterende nødrutiner i stor eller middels grad vurderes til å redusere fare for svikt i helsetjenesten må sees i sammenheng med andre svar i kartleggingen. Flere virksomheter nevnte varighet (tid) på IKT-bortfall som viktig risikofaktor for svikt i helsetjenesten. Generelt er det grunn til å anta at risiko for svikt i helsetjenesten øker betraktelig dersom nettverk feiler en lengre periode, og risiko øker dersom helsepersonell ikke har noen form for lesekopi av EPJ tilgjengelig.

Helsetilsynet spurte ikke om hvilken periode oppetiden måles, og ingen virksomheter har oppgitt tidsrom for prosentsatsene. For den som skal kjenne risikoen og lage egnede nødrutiner kan det være viktig om dette garanteres pr. uke, pr. måned eller pr. år. For eksempel betyr 99,9 prosent ca. 10 minutter pr. uke, men ca. 43 min. pr. måned og nærmere 9 timer på årsbasis. Risiko og behov for nødrutiner er ulik ved et stopp på 10 minutt og et stopp på 9 timer. Det kan virke som en ikke er fullt bevisst disse forskjellene. For øvrig er det ved noen foretak utfordringer med 'treghet' eller 'heng' i noen IKT-system. Dette er utfordrende å estimere og måle. Der foretakene oppgir 100 prosent oppetid (utover planlagte driftsbrudd) er det grunn til å anta at det mangler vurderinger, da 100 prosent oppetid generelt er lite sannsynlig for dagens IKT-løsninger.

3.3 Kommunikasjon rundt ØH-innleggelser og transport av akutt syke

3.3.1 Faktagrunnlag

3.3.1.1 Bortfall av 113

Tre av virksomhetene som svarte på undersøkelsen har egen AMK-sentral (Akutt Medisinsk Kommunikasjon) for øyeblikkelig hjelp (ØH). En av AMK-sentralene har skriftlige nødrutiner for bortfall av 113. De to andre foretakene svarte at de ikke har skriftlige nødrutiner for bortfall av 113.

På spørsmål om når foretakene sist testet nødrutiner for medisinsk nødtelefon 113 svarer ett foretak 2020, ett 2019 og ett før 2018.

Siden foretakene har testet nødrutine for 113 forstår vi at nødrutiner eksisterer.

Nødrutine for bortfall av 113 forutsetter bruk av andre IKT-system/ kommunikasjonsløsninger.

3.3.1.2 Amis

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 idag ved alle AMK-sentraler i landet. AMIS har funksjonalitet for mottak og registrering av nødmeldinger (inkl. opprinnelses-markering), bestilling av ambulansetransport, henvendelser til legevakt (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.

To av tre foretak har skriftlig nødrutine for Amis. Ingen av foretakene har svart på spørsmål vedrørende tidspunkt om når nødrutinen sist var testet. Ingen av de etablerte nødrutinene for Amis forutsetter bruk av andre IKT-system.

3.3.1.3 Koordinering av ambulanser ved hjelp av Transmed

Transmed brukes av alle ambulansesentraler for å holde oversikt over hvor ambulansene er og for å styre ambulansene.

«Nødrutiner for Nødnett hviler i stor grad på telefoni, og dette øker behovet for robuste telefoniløsninger.»

For to av de tre foretakene med AMK-sentral er det laget nødrutine for bortfall av Transmed. Det tredje foretaket oppgir at i praksis er «overgang til telefon» gjeldende nødrutine.

Et foretak oppgir å ha testet nødrutinen samme uke som de svarte på kartleggingen.

3.3.1.4 Nødnettet

Nødnett benyttes i virksomhetene ved AMK, ambulanse og akuttmottak, og at en virksomhet bruker Nødnettet for vektere og portører.

På spørsmål om hvert bruksområde har en nødrutine for bruk ved bortfall av Nødnett svarer fire av fem ja, og de har sendt inn gjeldende nødrutine. En virksomhet svarer nei på spørsmål om de har nødrutine for bruk ved bortfall av Nødnett.

Tre virksomheter har testet gjeldende nødrutine i perioden som kartlegging pågikk. De øvrige virksomhetene har ikke svart på spørsmål vedrørende testing. På spørsmål om nødrutinene forutsetter bruk av andre system svarer fire av virksomhetene at kombinasjoner av telefoni, mobiltelefon og satellittelefon brukes.

3.3.2 Refleksjoner, vurderinger av funn

Alle AMK-sentralene har nødrutine for medisinsk nødmeldetjeneste.

Nødrutinen for to virksomheter er overføring av medisinsk nødmeldetjeneste til andre sykehus i regionen. Siden foretakene deler mange regionale løsninger er det en svakhet i kartleggingen at det ikke er spurt om de har vurdert risiko for at virksomhetene som skal overta medisinsk nødtelefon har samme type feil samtidig. Ingen av de innsendte nødrutinene viser til samarbeid utover egen region.

Nødrutiner for Nødnett hviler i stor grad på telefoni, og dette øker behovet for robuste telefoniløsninger.

«Flere virksomheter sa det ville være vanskeligere å holde oversikt over pasienter jo lengre IKT-feil vedvarte.»

3.4 Diagnostisering av akutt syke ved IKT-bortfall

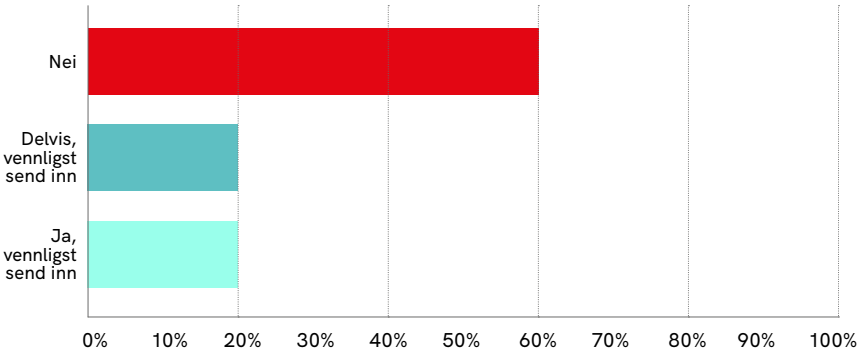
3.4.1 Faktagrunnlag

3.4.1.1 Oversikt over pasienter ved bortfall av IKT

Virksomhetene ga følgende svar vedrørende pasientoversikter ved IKT-feil:

Figur 3 Oversikt over pasienter

Sørger nødrutiner for at det finnes en oppdatert oversikt over inneliggende og planlagte pasienter ved bortfall av det pasientadministrative systemet?



En virksomhet svarte at de har pasientoversikter for innlagte pasienter på lokale datamaskiner.

Virksomheten som har «delvis oversikt» over pasienter tar hver morgen ut papirlister med pasientlister på poliklinikker og sengeposter. En tilsvarende mulighet hadde nok et av de øvrige sykehusene hatt på lokal beredskaps-pc også, men de sa selv at slike løsninger ikke er tilfredsstillende.

En virksomhet baserte midlertidige oversikter på fysiske tavler på sengeposter, papirkurver og utskrift av pasientlister (inneliggende) som ble tatt ut hver natt.

Flere virksomheter sa det ville være vanskeligere å holde oversikt over pasienter jo lengre IKT-feil vedvarte.

3.4.1.2 Oppetid og overordnet nødrutine for EPJ

EPJ (elektronisk pasientjournal) brukes her i betydning DIPS og DocuLive EPR. Alle virksomhetene har etablert overordnet nødrutine for dokumentasjon ved bortfall av EPJ. En virksomhet har rutiner for bruk av frittstående diktafoner som kan brukes ved IKT-feil.

Formål som er oppgitt i de fleste nødrutinene for EPJ er dokumentasjon av gitt helsehjelp. Ett foretak har oppgitt forsvarlig helsehjelp som hensikt med nødrutine for EPJ. Midlertidig dokumentasjon av journalopplysninger er fokus i rutinene. Ved to virksomheter står det beskrevet hvordan utskrift av journal kan hentes ved driftsstans i EPJ. Ved to foretak står det at lesekopi av EPJ vil bli gjort tilgjengelig dersom det er mulig, og dette er det nærliggende å anta gjelder for alle foretak. Hvor raskt det er mulig å sette opp lesekopi ved driftsstans (som ikke er planlagt) er uklart hos mange. Eventuell klargjøringer av lesekopier før IKT-endringer med risiko, og beslutningsstruktur for dette er også uklart hos mange.

Overordnet innhold i nødrutiner er:

Tabell 3 Alternativer til EPJ

Virksomhet 1	Virksomhet 2	Virksomhet 3	Virksomhet 4	Virksomhet 5
Fokus på varslingsrutiner og registrering av journal-dokumentasjon.	Fokus er å sikre livsnødvendig behan-dling og dokumentas-jon av gitt helsehjelp.	Fokus er å sikre registrering av journaldata.	Fokus på dokumentering av journalinformasjon.	Fokus er å sikre doku-mentasjon når DIPS er ute av drift.
DIPS vil bli satt i lesemodus (for alle pasienter) hvis det er mulig.	Dersom helse-nettet er oppe vil Docu-Live-leseserver (for alle pasienter) være tilgjengelig i løpet av ca. 1 time etter at HEMIT har fått melding.	Lesekopi står bare som et alternativ under planlagt nedetid (ikke ved ikke-planlagt driftsstans). Perma-nent nødrapport gir noe journalinformasjon fra DIPS om inne-liggende pasienter. Lokal back-up inne-liggende pasienter Meona tilgjengelig.	Utskrift av DIPS (alle pasienter) kan ved behov hentes på Driftssentralen. Lokal back-up inneliggende pasienter fra MetaVision tilgjengelig.	Står oppgitt ulike alternative prosedyrer dersom DIPS er i lese-modus versus at DIPS ikke er tilgjengelig i det hele tatt. Bruker (foreløpig) papirkurve som nødrutine/tilgang til viktig pasient-informasjon inne-liggende pasienter.

Ingen av nødrutinene for midlertidig journaldokumentering forutsetter bruk av nettverk.

Flere virksomheter mangler journalinformasjon om nye pasienter ved uforutsette EPJ-bortfall.

En region arbeider med å sette opp en permanent lesekopi av EPJ som back-up for uforutsette driftsproblem med EPJ.

Fire av virksomhetene svarte at de testet nødrutinen for EPJ i samme periode som de svarte på kartleggingen. En av virksomhetene hadde siste test av nødrutinen november 2018.

«Det å ha tilgang til helseopplysninger kan være avgjørende for å gi forsvarlig helsehjelp.»

3.4.1.3 Bestilling/svar på blodprøver når IKT-løsningene ikke fungerer

Fire av virksomhetene svarer at eksisterende nødrutiner sørger for sikker og effektiv bestilling/svar på blodprøver når IKT-løsningene ikke fungerer. En virksomhet svarer at nødrutiner delvis sørger for sikker og effektiv bestilling/svar på blodprøver når IKT-løsningen ikke fungerer.

Virksomhetene har sendt inn relevante nødrutiner.

3.4.1.4 Bestilling/svar på røntgenundersøkelser når IKT-løsningene ikke fungerer

Alle de fem virksomhetene som var med i kartleggingen svarte at de har nødrutine for bruk ved bortfall av røntgensystemet, inklusive bestilling av røntgenundersøkelser. Virksomhetene har også sendt inn gjeldende nødrutiner.

Fire av fem virksomheter har testet nødrutinene for røntgensystem siste år.

Fire av fem virksomheter svarer at nødrutine ikke forutsetter bruk av andre system. En virksomhet svarer at nødrutine er avhengig av e-henvisning (samme løsning som brukes av primærhelsetjenesten for å bestille røntgen).

3.4.2 Refleksjoner, vurdering av funn

Flere virksomheter sa det ville være vanskeligere å holde oversikt over pasienter jo lengre IKT-feil vedvarte. Dette fremgikk også av innsendte nødrutiner, og mediasaker har vist at planlagte pasienter raskt blir sendt hjem dersom IKT-systemene feiler. Da har ikke helsepersonell tilstrekkelig oversikt og journalinformasjon til å gi helsehjelp.

Det å ha tilgang til helseopplysninger kan være avgjørende for å gi forsvarlig helsehjelp. Alle helseforetak har mangelfull tilgang til journalinformasjon ved uforutsette IKT-bortfall. Mulige eksempel på løsninger for å sikre tilgang på helseopplysninger kan være å etablere kontinuerlig oppdatert lesekopi tilgjengelig for å kunne lese i EPJ ved IKT-feil. Lesekopi av EPJ kan trolig lages på ulike måter. Det er mulig å sette opp lokale elektroniske rapportuttrekk (alle pasienter) eller kopi av EPJ som kan benyttes uten sentralt nettverk.

Tilgang til EPJ kan også teoretisk løses ved registreringspraksis som sikrer at tilstrekkelig journalinformasjon er lagret i Kjernejournal, og at Kjernejournal også er tilgjengelig ved interne IKT-bortfall. Eller det kan være etablering av en nødrutine som sikrer tilgjengelige, oppdaterte og oversiktlige utskrifter fra EPJ ved IKT-bortfall.

Det er ikke direkte spurt om hvor lang tid det tar å etablere en lesekopi av EPJ ved uforutsette feil. Beslutningsprosessen for etablering av ›

«Det er bra at alle virksomhetene har nødrutiner for å ta blodprøver og bildeundersøkelser.»

lesekopi for EPJ er heller ikke kartlagt, og videre arbeid med lesekopi for EPJ anbefales i videre tilsynsarbeid. Generelt vil lesekopi for EPJ være et viktig tiltak for å sikre forsvarlig helsehjelp ved IKT-feil.

Det er bra at alle virksomhetene har nødrutiner for diagnostisering med blodprøver og bildeundersøkelser. Detaljer i nødrutinene er ikke vurdert.

3.5 Forsvarlig tildeling av legemiddel ved bortfall av IKT

3.5.1 Faktagrunnlag

3.5.1.1 Elektronisk medikamentkurve

To av virksomhetene som svarte på kartleggingen benytter elektronisk legemiddelkurve ved de fleste kliniske avdelinger i virksomheten. Et foretak har elektronisk legemiddelkurve på noen spesialavdelinger.

De to virksomhetene som har innført elektronisk kurveløsning på de fleste avdelingene har også etablert nødrutiner for bruk ved bortfall av systemene. Hver enhet har lokal back-up som sikrer tilgang til oppdatert oversikt over hvilke legemidler pasient har fått og hvilke legemidler som er ordinert. Disse virksomhetene hadde også testet nødrutinene sine under kartleggingsperioden.

For en virksomhet med kurveløsning på spesialenheter er det ikke sendt inn noen nødrutine.

3.5.2 Refleksjoner, vurdering av funn

Vurdert ut fra tilsendte svar i kartleggingen, har virksomheter med utbredt elektronisk legemiddelkurve nødrutiner for å ivareta forsvarlig legemiddeltildeling ved IKT-bortfall. Tilgang til kurve er vesentlig for pasientsikkerhet for inneliggende pasienter, og kan være viktigere for inneliggende pasienter enn EPJ ved bortfall av IKT. Dersom DIPS/DocuLive faller bort kan det å ha tilgang til kurveopplysninger være kritisk.

Overføringer av legemiddelinformasjon mellom ulike papir- og/eller elektroniske kurver er en kjent risiko. Denne risikoen er ikke vurdert.

3.6 Intern kommunikasjon/koordinering i sykehuset ved IKT-bortfall

3.6.1 Faktagrunnlag

3.6.1.1 Beredskapsorganisasjon

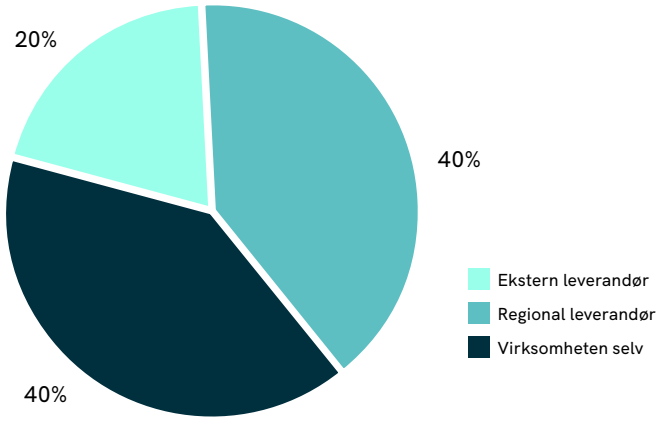
Alle virksomheter oppgir at de har en definert beredskapsorganisasjon for bortfall av IKT. Tre virksomheter benytter den generelle beredskapsorganisasjonen ved bortfall av IKT og utvider denne med IKT-leder ved behov.

Ved store IKT-utfordringer kommuniserer to virksomheter med IKT-driftsleverandør via egen IKT-beredskapsleder, to kommuniserer via ledere av beredskapsorganisasjonene og en virksomhet benytter en kombinasjon av disse.

3.6.1.2 Analogtelefon, IP-telefon eller DECT

Fire av fem virksomheter har en nødrutine for bruk ved bortfall av analogtelefon, IP-telefon og/eller DECT. Ansvar for drift av telefoniløsningene varierer noe mellom ekstern leverandør (en virksomhet), regionale leverandører (to virksomheter) og virksomheten selv (to virksomheter), se figur 4:

Figur 4 Ansvar for telefoniløsninger



To virksomheter har svart på spørsmål om når nødrutine for analogtelefon, IP-telefon og/eller DECT sist ble testet. De svarte at test ble utført i samme periode som denne kartleggingen (januar 2020).

På spørsmål om nødrutinene forutsetter bruk av andre IKT-system/kommunikasjonsløsninger svarte fire av virksomhetene ja. De listet opp ›

kommunikasjonsløsninger som mobiltelefon, IP-telefon gjennom Skype, Nødnett, satellittelefon, personsøkere, høytafoner og Ascom akuttvarsling.

3.6.1.3 Mobilnett

Fire av fem virksomheter svarer at de har en nødrutine for bruk ved bortfall av mobilnettet, og sendte inn gjeldende rutine. Felles for alle de innsendte nødrutinene er at de er svært overordnet og ingen har bruk av Telia eller ICE sine nett som alternativ nødløsning i forhold til Telenor, som de har valgt som hovedleverandør.

Ingen har rutiner for innkalling av bakvakter når hovedleverandørens mobilnett svikter. To av virksomhetene svarte at nødrutinen delvis sikrer at bakvakter kan kalles inn når hovedleverandørens mobilnett er ute av drift, men at det er mye vanskeligere.

Bare en av virksomhetene svarte på spørsmålet om når nødrutinen sist ble testet, de hadde testet nødrutinene sine i 2016. På spørsmål om nødrutinen forutsetter bruk av andre IKT-system svarte fire virksomheter at de forutsetter bruk av løsninger som IP-telefoni, Skype, Nødnett, satellittelefon, fasttelefon IP, fasttelefon digital, mobilix-meldingsvarsler på mobiltelefoner over wifi og personsøkere.

3.6.1.4 Sykesignalanlegg

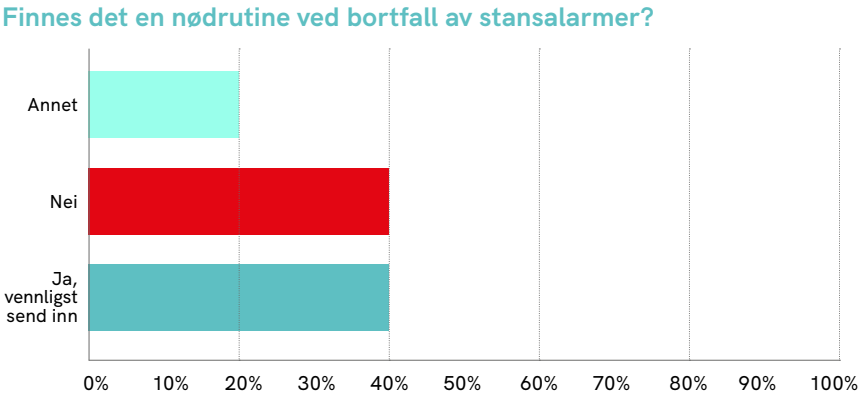
Fire av de fem virksomhetene har ansvar for driften av sykesignalanlegget og stansalarmene selv. Ved en virksomhet har det regionale IKT-driftsselskapet ansvar for driften av sykesignalanlegget og stansalarmene.

En virksomhet oppgir opp-bemanning i klinikkene som nødrutine ved feil i sykesignalanlegg. Tre virksomheter er uten nødrutine ved feil i sykesignal og en virksomhet har sendt inn en nødrutine som hovedsakelig innebærer åpne dører inn til pasienter ved feil i sykesignalanlegg. På spørsmål om når nødrutine for bruk av bortfall av sykesignalanlegg sist ble testet er det to virksomheter som har svart.

3.6.1.5 Stansalarmer

Vedrørende nødrutine for bruk ved bortfall av stansalarmer har virksomhetene gitt følgende svar:

Figur 5 Nødrutine for stansalarmer



Kommentar sendt inn fra en virksomhet (Annet): «Nødrutine er å ringe 113 som varsler, bruke høytafon.»

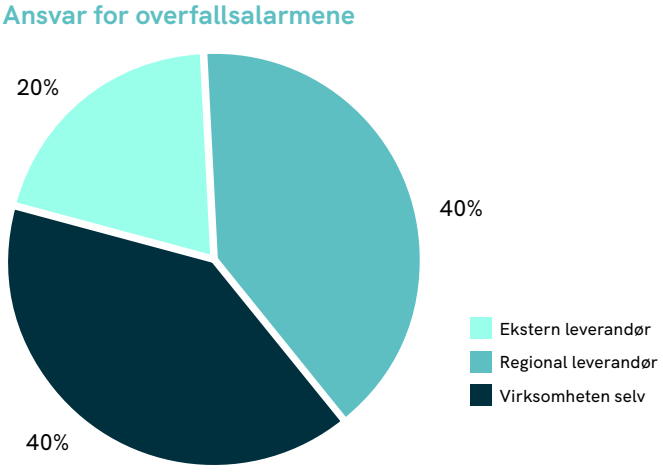
Fire av fem virksomheter har testet nødrutinen for stansalarmer i perioden som kartlegging pågikk (hvorav en virksomhet har automatisk test av stansalarm hver morgen), en virksomhet svarer at de sist testet nødrutinen i 2016.

Tre virksomheter svarer at nødrutinen for stansalarm forutsetter bruk av andre IKT-system/kommunikasjonsløsninger. Løsninger som de bruker i nødrutiner er telefon/mobiltelefon, høytafon og høyttalere som tilhører brannvarsling.

3.6.1.6 Overfallsalarmer

Ansvar for drift av overfallsalarmene varierer noe mellom ekstern leverandør, regionale leverandører og virksomheten selv:

Figur 6 Drift av alarmer



> «Det vil være en betydelig risiko for helsehjelpen dersom sykesignalsystem ikke fungerer og bare skal erstattes av åpne dører inn til pasientrom.»

Overfallsalarmer brukes ved psykiatriske avdelinger i alle virksomhetene, i akuttmottak i tre virksomheter, samt at overfallsalarmer benyttes av renholdere i en virksomhet. En virksomhet har mer utstrakt bruk av overfallsalarmer klinisk og administrativt.

Tre av virksomhetene har nødrutiner for bruk ved feil i overfallsalarmer. Tre av virksomhetene oppgir at de bruker annen teknologi ved eventuelle feil i overfallsalarmer. Alternativer som er oppgitt er mobiltelefon, DECT/ ASCOM-telefoner, Securitas-alarm og høyttalere som tilhører brannvarsling.

3.6.2 Refleksjoner, vurderinger av funn

Erfaring fra flere tilsynssaker har vist at velfungerende kommunikasjonsløsninger internt i sykehus kan være avgjørende for å gi forsvarlig helsehjelp. Det kan ut fra kartleggingen se ut til at det er etablert færrest skriftlige nødrutiner og tester av nødrutiner for kommunikasjonsløsninger (sammenlignet med øvrige områder som er kartlagt). Sykesignalsystem med alarm fra kritisk syke til helsepersonell, og velfungerende koordinering av helsepersonell som behandler akutt syke er viktig for å kunne gi forsvarlig helsehjelp, og forutsetter robuste system. Det vil være en betydelig risiko for helsehjelpen dersom sykesignalsystem ikke fungerer og bare skal erstattes av åpne dører inn til pasientrom.

Helseforetak som benytter regional driftsleverandør har (utfra foreløpige funn i beslutningsstruktur for risikovurderinger her) trolig mindre myndighet over løsningene.

Telenors mobilnett har vært ute av drift flere ganger, slik at foretakene burde ha registrert en ikke-planlagt 'test' på mobilløsninger her.

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

3.7.1 Faktagrunnlag

3.7.1.1 Kjennskap til nødrutiner hos ansatte

På spørsmål om hvordan virksomhetene lagrer nødrutiner for å sikre at de er tilgjengelige også ved bortfall av nettverk svarte virksomhetene slik:

Tabell 4 Lagring av nødrutiner

Hvordan lagres nødrutiner for å sikre at de er tilgjengelige også ved bortfall av nettverk?
Nødrutiner er skrevet ut og lagres samlet i en perm. Perm oppbevares i områder som vaktrom eller tilsvarende i de forskjellige avdelingene.
Papirkopi nødstrøm på servere for å hente ut nødrutiner lokal tilgang til server.
Lokalt per enhet men det er sentral løsning under etablering (papir i beredskapsperm på servicesenter).
Utskrift av alle nødrutiner er lagret i permer pr avd. Alle ansatte er informert hvor den står.
I egne beredskapspermer plassert på strategiske steder på Sykehuset.

De fleste sykehus oppgir at de har nødrutiner skrevet ut på papir som er lagret i egne beredskapspermer på kliniske avdelinger.

På spørsmål om hvordan nødrutiner blir gjort kjent for nyansatte og kontinuerlig opplyst om i organisasjonen svarte alle at nyansatte får opplæring eller at de gjorde nødrutiner kjent ved planlagt nedetid.

Flere virksomheter gjorde nødrutiner kjent gjennom elektroniske læringsportaler og kvalitetssystem, ved utsendelser ved planlagte driftsstans og en virksomhet hadde lagt nødrutiner inn som en del av lederopplæringsprogram. I tillegg svarte en del av virksomhetene at ledere på ulike enheter har laget nødrutiner og struktur for opplæring. En virksomhet la ut nødrutinen sin for pasientsignal i felles katalog for nødrutiner i kartleggingsperioden.

Kontaktpersoner for virksomhetene fortalte at ledere på ulike nivå er ansvarlige for å utarbeide nødrutiner for de område de har ansvar for, og ledere har noe ansvar for opplæring. Oppfølging av dette ansvaret kan variere noe og ble ikke videre undersøkt.

3.7.1.2 Oppdatering av nødrutiner

På spørsmål om virksomhetene sørger for jevnlig forbedring/ oppdatering av nødrutiner svarte tre virksomheter ja, en virksomhet delvis og en virksomhet nei. En virksomhet har sendt inn overordnet beskrivelse for oppdatering av rutiner. Flere foretak har automatisk varsling til rutineansvarlig i kvalitetssystemet når ulike nødrutiner skal oppdateres.

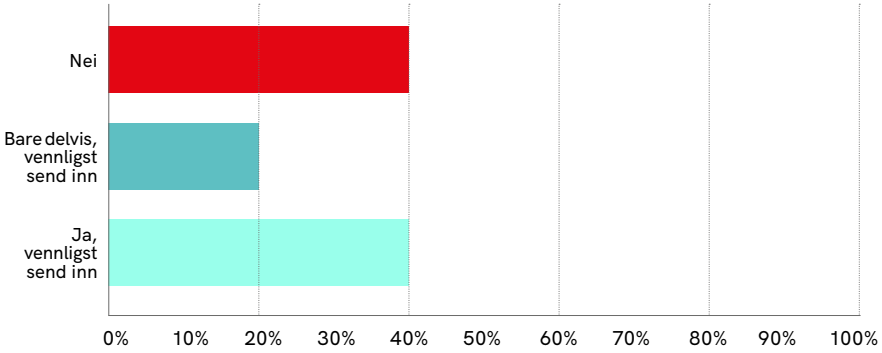
Som grunnlag for oppdatering av nødrutiner, ble virksomhetene stilt spørsmål om avvik i pasientbehandling som skyldes bortfall av IKT.

«Generelt virker det som om informasjon fra avviksrapporterings-systemet i liten grad brukes til systematisk forbedring på IKT-området.»

En virksomhet hadde en slik rapport med avvik for de siste tre år. En virksomhet lagde en tilsvarende rapport mens kartleggingen pågikk. To virksomheter var uten slike rapporter, og en virksomhet hadde delvis oversikt over avvik ved at IKT-sikkerhetsleder fulgte opp slike avviksmeldinger etter hvert som de ble meldt inn fra brukere.

Figur 7 Oversikt avvik

Har virksomheten oversikt over avvik i pasientbehandling som skyldes bortfall av IKT?



Ingen av virksomhetene har sendt inn rutiner for oppdatering av nødrutiner som innebærer tydelig oppfølging av avvik i pasientbehandlingen som følge av IKT-bortfall.

3.7.2 Refleksjoner, vurderinger av funn

Det virker som helsepersonell har nødrutiner tilgjengelig i egne beredskapspermer med papir når IKT faller bort (ikke validert med kliniske avdelinger).

Generelt virker det som om informasjon fra avviksrapporterings-systemet i liten grad brukes til systematisk forbedring på IKT-området. Dette kan ha sammenheng med generell kultur for avviksrapportering, brukervennlighet i avvikssystem, utfordringer med avviksrapporter, manglende tilbakemelding til melder, meldingstretthet eller lignende.

4

Litteraturliste

1. Utviklingstrekk 2020. Drivere og trender for e-helseutviklingen. Oslo, Direktoratet for e-helse, 2020.
2. Varsel om vedtak – overtredelsesgebyr – Sørlandet Sykehus HF. Brev fra Datatilsynet til Sørlandet sykehus HF, 24.10.2017. (Ref. Datatilsynet 16/01531-45/GRA)
3. Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen). Versjon 6.0. Vedtatt 4. februar 2020.
4. EPJ standard. Tilgangsstyring, retting og sletting. (Teknisk standard nr. HIS 80506:2019.) Oslo: Direktoratet for e-helse, 2019.
5. Nasjonal strategi for informasjonssikkerhet. Oslo: Fornyings-, administrasjons-, og kirkedepartementet, 2012.
6. Meld. St. 38 (2016–2017). IKT-sikkerhet – Et felles ansvar.
7. Datatilsynet. Iverksette styringssystem for informasjonssikkerhet. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/?id=11147 / Lest 1.1.2020.

Øvrig litteratur

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

ITIL. The IT Service Management. Forum AXELOS Community Page https://www.itsmfi.org/page/AXELOSCommunityPage / Lest 1.1.2020

Metodebibliotek for IKT-arbeid i spesialisthelsetjenesten https://kilden.sykehusene.no/ Lest 1.1.2020.

5 Vedlegg: Ordliste, begrepsbruk

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. (3)

Databehandler
Databehandler er den som behandler helse- og personopplysningene på vegne av den dataansvarlige, jf. Personvernforordningen artikkel 4 nr. 8. (3)

EPJ – Elektronisk PasientJournal
Elektronisk ført samling eller sammenstilling av nedtegnede/registrerte opplysninger om en pasient i forbindelse med helsehjelp (4).

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. (3)

IKT-sikkerhet
Integritet, konfidensialitet og tilgjengelighet er viktige sikkerhetsmål når det gjelder å ivareta IKT-sikkerhet (5).

- 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. (6)

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.

Informasjonssikkerhet
Informasjonssikkerhet handler om å bevare informasjonens konfidensialitet, integritet og tilgjengelighet. I tillegg har Datatilsynet definert informasjonssikkerhet til også å inkludere robusthet (7).

Klinisk IKT-system
Et elektronisk behandlingsrettet helseregister.

Konfidensialitet
Krav om konfidensialitet innebærer at informasjon ikke blir kjent for uvedkommende (ikke-autoriserte 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.

PAS
Pasientadministrativt system (i praksis har alle virksomheter et felles system for PAS/EPJ per 2019/2020).

Risikovurdering
Risikovurdering er et begrep i risikostyringen som dekker de tre stegene risikoidentifisering, risikoanalyse og risikoevaluering, se kap. 2.2.

Røntgensystem (PACS/ RIS)
(Picture Archiving and communication system) bildearkivsystem. Samordnes etterhvert i større grad med multimediaarkiv.
RIS: Røntgeninformasjonssystem.

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

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.)

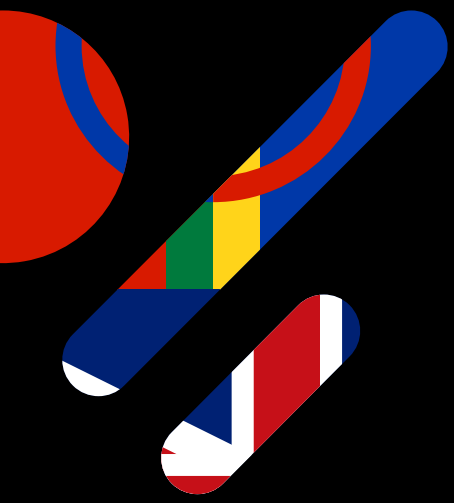
Tilgjengelighet
Krav om tilgjengelighet innebærer at informasjon skal være tilgjengelig og anvendelig når den autoriserte ber om det.

Øvrige definisjoner se Norm for informasjonssikkerhet

https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgstjenesten#6.1%20Definisjoner>

6

Samisk og engelsk sammendrag



Mo leat buohcciviesut ráhkkanan jus IKT-jávká?

Viđa doaimmahaga kárten

ČOAHKKÁIGEASSU DEARVVAŠVUOĐABEARRÁIGEAHČU RAPORTA 3/2020:S

2019/2020 dálvvi čađahii Stáhta dearvvasvuođabearráigeahčču kártema viđa doaimmahaga oppalašgovas kritihkalaš vuogádagain, riskaárvvoštallamiin ja heahterutiinnain mat sis leat IKT-vuogádagaide. Kárten lea ráddjejuvvon moatti doaimmahahkii spesialistadearvvašvuođabálvalusas. Sáddejuvvon vástádusain ii leat dahkkon lobálašvuođadárkkisteapmi. Dán raporttas lea čoahkkáigeassu das ja ovdanbuktit daid deháleamos gávdnosiid.

Doaimmahagat leat buori muddui identifiseren guđemuš IKT-vuogádagat leat kritihkalačča t, ja buori muddui ráhkadan heahterutiinnaid guovddáš funkšuvnnaide nu mo diŋgot iskkademiid ja dálkasiid juohkit. Leat dattege unnán doaimmahagat mat nagodit bisuhit oppalašgova pasieanttain mat leat sisačálihuvvon ja plánejuvvon jus IKT-jávká. Mađi guhkit áigodaga boasttuvuohta IKT:s bistá, dađi stuorát riska lea ahte šaddá váilevašvuohta dohkálaš dearvvašvuođabálvalusain. Pasieanttat geat bohtet fáhkkatlaš dikšui go journálavuogádagat eai leat olámuttos, fertejit oalle muddui dikšojuvvot dieđuid haga ovdalis divššu birra.

Mearridanstruktuvrrat mat gullet EPJ lohkankopiijaid (elektronalaš beassan lohkat elektronalaš pasieantajournálaid back-up:id) ásaheapmái leat máŋgga doaimmahagas eahpečielgasat. Ii lean áibbas čielggaduvvon, gaskal muhttin dearvvašvuođadoaimmahagaid ja IKT-bálvalusfitnodagaid, geas lea ovddasvástádus čađahit ja dohkkejit riskaárvvoštallamiid.

Doaimmahagat celket ahte heahterutiinnat leat sestojuvvon sierra gearggusvuođapearpmaide klinalaš ossodagain. Leat veahá erohusat heahterutiinnaid hárjehallamiin, muhto duohtavuođas šaddá heahterutiinnaid iskkus dalle go leat duohta doaibmaváttisvuođat. Raporta addá vuođu viidát kártemii. Diehtosihkarvuođas guorahallo beasatlašvuohta, muhto ii konfidensialitehta iige integritehta.

How have hospitals prepared for the possible loss of ICT systems?

Survey of five enterprises

REPORT OF THE NORWEGIAN BOARD OF HEALTH SUPERVISION 3/2020

During the winter 2019/2020, the Norwegian Board of Health Supervision conducted a survey of five enterprises and their overview of critical systems, risk assessments and emergency procedures regarding ICT systems. The survey was limited to a number of enterprises within the specialist health service. No legality checks were carried out on the responses that were received. In this report, we present the key overall findings.

The enterprises have mostly identified the ICT systems that are critical, and largely developed emergency procedures for key functions, such as the ordering of tests/investigations and the distribution of medicines. However, few enterprises would be able to maintain an overview of admitted and scheduled patients in the event of a loss of ICT. The risk of failure of proper healthcare also increases the longer period of ICT failure lasts. Patients arriving at an A&E department while the medical record system is unavailable would largely have to be treated without any information concerning previous treatment.

Several enterprises have unclear decision-making structures concerning the establishment of read-only copies of EMR (electronic access to read back-up electronic patient records). There was some unresolved delegation of responsibilities between some health enterprises and ICT providers regarding the preparation and approval of risk assessments.

The enterprises stated that emergency procedures are stored in separate emergency folders in clinical departments. There is some variable practising of emergency routines, but in practice emergency routines will be tested in the event of real operational problems. The report forms the basis for a wider survey. Information security is investigated as regards accessibility, but not as regards confidentiality or integrity.

Mer om IKT-tilsyn på www.helsetilsynet.no

Helsetilsynets «IKT-tilsyn» – normen(es) vokter og helse-arbeidernes 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 978-82-93595-33-5
Rapport fra Helsetilsynet 3/2020.
Hvordan er sykehusene forberedt på IKT-bortfall? Kartlegging ved fem virksomheter, elektronisk versjon.

Kartlegging ved fem virksomheter

Hvordan er sykehusene forberedt på IKT-bortfall?

RAPPORT FRA HELSETILSYNET 3/2020 • AUGUST 2020

Statens helsetilsyn gjennomførte vinteren 2019/2020 en kartlegging av fem virksomheter sine oversikter over kritiske system, risikovurderinger og nødrutiner for IKT-system. Kartleggingen er avgrenset til noen virksomheter i spesialisthelsetjenesten. Det er ikke gjort en lovlighetskontroll av innsendte svar. I denne rapporten gir vi en samlet presentasjon av de viktigste funnene.

Virksomhetene har i stor grad identifisert hvilke IKT-system som er kritiske, og i stor grad utarbeidet nødrutiner for sentrale funksjoner som bestilling av undersøkelser og utdeling av legemiddel. Det er imidlertid få virksomheter som klarer å holde oversikt over inneliggende og planlagte pasienter ved IKT-bortfall. Fare for svikt i forsvarlige helsetjenester øker dessuten jo lengre periode IKT-feil varer. Pasienter som kommer til akuttmottaket mens journalsystem er utilgjengelig, må i stor grad behandles uten informasjon om tidligere behandling.

Beslutningsstrukturer vedrørende etablering av lesekopier av EPJ (en elektronisk tilgang til å lese back-up av elektronisk pasientjournal) er uklare ved flere virksomheter. Det var noe uavklart ansvar mellom noen helseforetak og IKT-driftsleverandører vedrørende utføring og godkjenning av risikovurderinger.

Virksomhetene oppgir at nødrutiner er lagret i egne beredskapspermer på kliniske avdelinger. Det er noe varierende øving i nødrutiner, men i praksis får en test av nødrutiner ved reelle driftsproblem. Rapporten danner grunnlag for en større kartlegging. Informasjonssikkerhet undersøkes for tilgjengelighet, men ikke for konfidensialitet eller integritet.

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