

Risikovurderinger, nødrutiner og
forbedringsarbeid ved 17 sykehus

Forsvarlig pasient- behandling uten IKT?



Helsetilsynet

TILSYN MED BARNEVERN,
SOSIAL- OG HELSETJENESTENE

RAPPORT 2/2021 • APRIL 2021

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 «En 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 kommunikasjonsentral) i annen region.

Personvern hensyn vektes ikke mot krav til forsvarlig helsehjelp

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

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.

informasjon for høyt liggende pasienter ved bortfall av EPJ, og vurdere lignende backupløsninger for nøkkelpersonell som koordinatorene i sentraloperasjoner eller lignende

er viktig informasjon i ulike systemer) 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)

innses et godt kommunikasjonskanaler som forutsetter IKT-nettverk eller ordinære telefonsamband

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 ansvars plassering i alle ledd fra innkjøp til avviking.

Noen virksomheter:

pasienter ved IKT-bortfall

av dpp og elektronisk legemiddelkurve

etse Vest s er et a (utført 1.1.21 red.anm.)

via elektronisk kurve eller AMIS (der API er utviklet)

meldings- og ta e 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 ●

