Felles kommunal journal interim AS

Bilag 5.2:

Overordnet risikovurdering

Styringsdokument

Felles kommunal journal: Et felles journalløft for kommuner utenfor helseregion i Midt-Norge

Versjon 0.8

18.11.2022

INNHOLDSFORTEGNELSE

1. INNLEDNING 1

2. OMFANG OG AVGRENSNINGER 1

3. BESKRIVELSE AV LØSNING OG VERDIER: 2

3.1. Tilgang til relevant pasientinformasjon 2

3.2. Hvor vil informasjonen behandles? 3

4. VURDERING AV IDENTIFISERTE RISIKO OG HENDELSER 3

4.1. Vurdering av identifiserte risikoer knyttet til konfidensialitet 4

4.2. Vurdering av identifiserte risikoer knyttet til integritet 6

4.3. Vurdering av identifiserte risikoer knyttet til tilgjengelighet 6

4.4. Vurdering av identifiserte risikoer knyttet til personvern/GDPR 8

4.5. Vurdering av identifiserte risikoer knyttet til drift og forvaltning av IKT-funksjoner 9

5. EVALUERING AV RISIKO 11

5.1. Eksempel på tiltak for hendelser med kritisk/høy risiko 11

5.2. Eksempel på tiltak for hendelser med moderat risiko 15

6. VIDERE ARBEID MED RISIKO 20

7. UNDERLAG 0

7.1. Risiko- og sårbarhetsanalyse 0

7.2. Definisjoner i Risiko- og sårbarhetsanalyse 9

1. INNLEDNING

I dette bilaget finner du:

- Overordnet beskrivelse av løsning
- Vurdering av identifiserte risikoer og hendelser
- Eksempler på sentrale tiltak for å imøtekomme risikoene identifisert

Bilaget hører til Vedlegg 5. Det kan også sees i sammenheng med Bilag 5.1.

Risikovurdering er et verktøy vi bruker for å identifisere uønskede hendelser, og analysere konsekvens og sannsynlighet. Risiko er knyttet til mulige avvik fra våre mål, ønskede resultater eller ønskede tilstander[1]. Til en risikovurdering følger alltid tiltak for å redusere eller fjerne detekterte risikoer.

På nåværende tidspunkt gjøres en overordnet risikovurdering. Det bør likevel anvendes som en sentral aktivitet for å få frem sentrale risiko og tiltak som må innarbeides fortløpende gjennom hele arbeidet. Risikovurderingen er gjennomført av kommunale ressurser i prosjektet. Dette har vært viktig for å sikre erfaring og forankring til en kommunal virkelighet og utfordringsbilde.

Tiltaket omfatter flere ulike aktører. Det er kommunene som virksomheter og som arbeidsgiver for helsepersonell, helsepersonell, innbyggere, leverandører og andre nasjonale aktører. Tiltaket omfatter øvrige kommuner (utenfor helseregion Midt-Norge), og det behandles informasjon om flere ulike sårbare grupper.

Norm for informasjonssikkerhet[2] («Normen») danner et grunnleggende rammeverk for ivaretagelse av informasjonssikkerhet i kommunene, og ligger til grunn for alt arbeid som gjøres i tiltaket sammen med Nasjonal Sikkerhetsmyndighet (NSM) sine grunnprinsipper for informasjonssikkerhet[3].

Det må gjøres nye risikovurderinger ved planlegging og gjennomføring av alle steg av utprøvinger.

2. OMFANG OG AVGRENSNINGER

Risikovurdering er avgrenset til å ikke omfatte markedsplassen ettersom den kun beskrives konseptuelt på nåværende tidspunkt. Tilsvarende vil ikke nasjonale samhandlingsløsninger være en del av omfanget i denne vurderingen.

I denne fasen har vi ikke detaljkunnskap om løsningselementene (plattform, understøttende IKT-infrastruktur samt applikasjonene som skal kjøres mot plattformen). Det medfører at overordnede betraktninger og vurderinger legges til grunn i vurderingen. Utviklingen av tiltaket skal være stegvis, og risikovurdering er gjort med utgangspunkt i en tenkt kommune slik at den kan brukes som grunnlag i forbindelse med utprøving.

Det forutsettes at det vil måtte gjøres ROS-analyser av de enkelte applikasjonene som tilgjengeliggjøres mot plattformen, samt etablering av plattformen med tjenester som realiseres. En ROS-analyse bør innebære detaljkunnskap om faktiske verdier, sårbarheter, tilsiktede trusler, utilsiktede farer og risiko. Dette må derfor gjennomføres i nær sammenheng med realisering, og også sees i nær sammenheng med personvernkonsekvensvurderinger (DPIA).

[1] Om risiko og risikovurdering | Digdir

[2] Normen - ehelse

[3] Grunnprinsipper for IKT-sikkerhet - Nasjonal sikkerhetsmyndighet (nsm.no)

3. BESKRIVELSE AV LØSNING OG VERDIER:

Det overordnede målbildet for prosjektet er etablering av et plattformbasert økosystem for aktører som helsepersonell, innbyggere, kommuner og leverandører. Via en felles logisk informasjonskilde (plattform) skal alle sikres tilgang til samme informasjon, på bakgrunn av tjenstlig behov. I tillegg til plattformen består løsningen også av en markedsplass, en møteplass for kunder og leverandører. Dette beskrives i vedleggene 2 – 4. I dokumentets kap 3.1 og 3.2 gis en kort oppsummering av deler av løsningsbeskrivelsen. I den grad det skal oppleves inkonsistens mot andre deler av styringsdokumentet er det styringsdokumentets kap 3 som er gjeldende.

3.1. Tilgang til relevant pasientinformasjon

Plattformen skal lagre og sammenstille relevant informasjon om mottagere[4] av kommunale helse- og omsorgstjenester. Dette betyr at det er sensitive personopplysninger[5] som håndteres i plattformen. Grad av sensitivitet er i denne sammenhengen også knyttet til informasjonens skadepotensial forbundet med brudd på informasjonens konfidensialitet, integritet eller tilgjengelighet.

Sluttbrukerløsningene, journalsystemene og applikasjonene, skal via plattformen benytte den samme informasjonen.

Omfanget for en plattform er innledningsvis avgrenset til å omfatte relevant pasientinformasjon (for mer informasjon om avgrensninger som er gjort se Vedlegg 4, samt Bilag 2.1). Prosjektet har arbeidet frem en avgrensning av hva et forventet omfang av informasjon kan være, innledningsvis. Det vises til Bilag 2.2 for utfyllende informasjon for beskrivelse av hva disse kategoriene er.

I målbildet vil informasjon lagres i en felles logisk informasjonskilde. Dette trenger ikke å være en fysisk database, men kan også være distribuerte plattformer som fungerer som en logisk plattform. Vi anbefaler at plattformen er skybasert og at kravet til journalleverandører også må være at de skal levere skybaserte løsninger.

Lagring av pasientinformasjon baseres på bruk av åpne internasjonale standarder (eksempelvis openEHR[6], HL7 FHIR[7] og SNOMED CT[8]) der det er mulig og hensiktsmessig. Dagens sluttbrukerløsninger (med integrert lokal lagring), må kunne sende og motta pasientinformasjon til og fra plattformen.

Plattformen vil ha et kommunikasjonslag med en oversikt over hvilke opplysninger som er lagret i de tilknyttede sluttbrukerløsningene, samt hva som fortsatt bør lagres lokalt og hvilke integrasjoner til andre systemer som er tilgjengelig.

For eksisterende EPJ-leverandører som ønsker å opprettholde lokal lagring som primær kilde vil det være mer hensiktsmessig å beholde brukerflate og lagring sammen lokalt, men gjøre det mulig å overføre informasjon til plattformen. Dette vil nødvendigvis innebære at man opererer med synkroniserte sett av samme informasjon.

---

[4] «Mottager» er i denne sammenheng innbyggere eller besøkende i kommunen som mottar kommunale helse- og omsorgstjenester

[5] Eksempler på sensitive personopplysninger er behandling av genetiske og biometriske opplysninger, helseopplysninger, opplysninger om en fysisk persons seksuelle forhold, eller seksuelle orientering mm

[6] openEHR er en e-helseteknologi bestående av åpne spesifikasjoner, kliniske modeller og programvare, som kan brukes til å lage åpne plattformer for helsevesenet

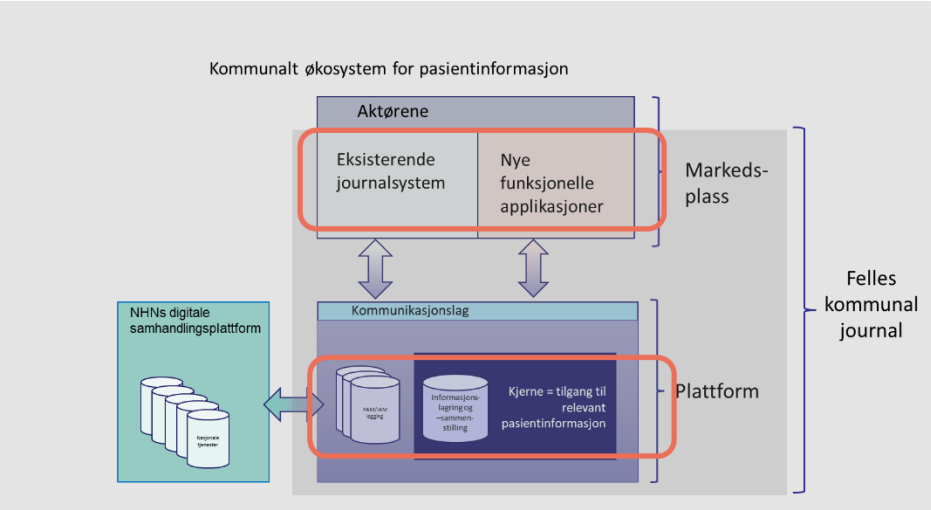
[7] HL7 FHIR er en fritt tilgjengelig standard som ble utarbeidet for å møte krav til integrasjon mellom virksomheter og mot moderne teknologi som mobil- og skytjenester. Vil bli brukt i nasjonale e-helseløsninger og har god støtte for interoperabilitet mellom virksomheter

[8] SNOMED CT er en omfattende terminologi som brukes til å beskrive kliniske konsepter. Den er valgt som standard i Norge og brukes i Helseplattformen

Det er ikke noe mål å lagre primærinformasjon eller kopier på plattformen, og i en skybasert verden vil utfordringene med tilgjengelighet kunne reduseres. På den annen side kan lagring i plattformen være en løsning for sluttbrukerløsninger som ikke selv lagrer informasjon. Vi forutsetter at de nasjonale løsningene støtter tilstrekkelig grunndata for plattformen. Det er også mulig at plattformen må tilby lagring av informasjon som nasjonale samhandlingsløsninger ikke har hjemmel til å fortsette å lagre (tidsavgrenset hjemmel), men som kommunene har plikt til å ta vare på i et lengre perspektiv.

3.2. Hvor vil informasjonen behandles?

Informasjon vil behandles både i plattformen (markert som plattform i figuren), samt i de ulike sluttbrukerløsningene (markert som eksisterende journalsystem og nye funksjonelle applikasjoner i figuren).



4. VURDERING AV IDENTIFISERTE RISIKO OG HENDELSER

I dag er det store variasjoner i ulike kommuners systemer, infrastruktur, teknologi og tilnærming til IKT-sikkerhet. Dette medfører uheldig kompleksitet i systemer og infrastruktur som kan påvirke informasjonssikkerhet og personvern i plattformen, eller deler av verdikjeden. Forholdene muliggjør en større mengde angrepsflater, som gir en eksponentiell vekst i behov for risikoreduserende sikkerhetstiltak for å sikre et forsvarlig sikkerhetsnivå i dagens systemer, infrastruktur og alle tilhørende teknologier.

Sentralisering av sikkerhetsfunksjoner er en viktig del av anerkjent beste praksis for IKT-sikkerhet, og bør legges til grunn i det overordnede målbildet. Det muliggjør en enhetlig tilnærming til autoriserte tilganger, med grunnlag i tjenstlig behov, og forsvarlig sikring av informasjon med grunnlag i en helhetlig sikkerhetsarkitektur[9]. Sentralisering av sikkerhetsfunksjoner og en enhetlig sikkerhetsarkitektur vil gi forutsetninger for felles tilnærming til beste praksis for informasjonssikkerhet og personvern.

Når kommuner tar plattformen i utstrakt bruk vil virksomhetene, samfunnet og enkeltpersoner være avhengig av at plattformen tilgjengeliggjør og behandler oppdatert og pålitelig informasjon i sine tjenester. Dette inkluderer informasjon i sluttbrukerløsningene (for eksempel EPJ-applikasjoner), informasjonstjenester, lagringstjenester samt andre tjenester som understøtter infrastruktur mm. Et

9 Se for eksempel Grunnprinsipp 2.1 i NSMs grunnprinsipper for IKT-sikkerhet.

brudd på informasjonens tilgjengelighet eller integritet kan være forbundet med et potensielt uakseptabelt skadepotensial. Spesielt fordi dette kan påvirke liv og helse direkte. Tilsvarende vil et brudd på konfidensialitet være forbundet med uakseptabelt skadepotensial, og plattformen forventes derfor å skulle skjerme sensitive opplysninger mot uvedkommende.

Med grunnlag i definisjon og forståelse av relevant pasientinformasjon kan det konkluderes med at en stor andel sensitive personopplysninger vil bli behandlet i plattformen. Grad av sensitivitet er i denne sammenhengen direkte knyttet til informasjonens skadepotensial og forbundet med brudd på informasjonens konfidensialitet, integritet eller tilgjengelighet. Sensitiv informasjon kan utnyttes av uvedkommende til å påvirke den operative evnen virksomhetene har når det gjelder beslutninger eller behandlinger, eller påvirke personers liv og helse direkte.

Første steg i risikovurderingen identifiserer risiko. Formålet er å lage en omfattende liste over mulige hendelser som kan føre til negative konsekvenser for evne til å utføre oppgaver og tjenester, ivareta plikter og økonomi[10]. Det andre steget analyserer risikoen, og utviklingen av en forståelse av risikoene. Formålet er å kunne fastslå mulig konsekvens og tilhørende sannsynlighet på hendelser identifisert i forrige steg. Dette gir en god beskrivelse av risiko[11]. Resultatene av disse aktivitetene presenteres i det følgende, med hovedfunnene innenfor områdene *konfidensialitet, integritet, tilgjengelighet, personvern/GDPR og drift/forvaltning.*

Kategorier og verdier presentert i figur er lagt til grunn i arbeidet. Fargene vil følge risikoverdi i beskrivelsene i kapitelet. Det vises også til slutten av bilaget for mer utfyllende forklaring av hva som er lagt til grunn som kriterier for vurdering av oppnådd verdi.

Risikoverdi = sannsynlighet * konsekvens

Risikoverdien vil være et tall mellom 1 og 25. Vi opererer med følgende tolkning av risikoverdien:

Lav risiko:	≤	Risikoverdi	≤	4		
Moderat risiko:	≤	Risikoverdi	≤	9		terskel for tiltak
Høy risiko:	≤	Risikoverdi	≤	16		
Kritisk risiko:	≤	Risikoverdi	≤	25		

Figur 1: Risikoverdier brukt i vurderingen

4.1. Vurdering av identifiserte risikoer knyttet til konfidensialitet

Konfidensialitet handler om å sørge for at informasjon ikke kommer i feil hender eller på avveie.

En av risikoene som er vurdert som høy er at informasjon, dvs. personopplysninger, kommer på avveie på grunn av teknisk sårbarhet. Dette kan skje av ulike årsaker, og noen eksempler er manglende kryptering av data (mulig å avlytte datatrafikk) eller teknisk sårbarhet i infrastruktur hos en av aktørene. Mange integrasjoner øker også risikoen. Vi scorer denne hendelsen høyt fordi det må tas hensyn til et stort aktør- og løsningsbilde som skal samspille, så vi forventer at slike hendelser derfor vil skje oftere enn i mindre og avgrensede miljø.

[10] Om risiko og risikovurdering | Digdir

[11] Om risiko og risikovurdering | Digdir

Tilsvarende er risikoen for informasjon på avveie på grunn av tilfeldig eller målrettet angrep vurdert som høy. NHO har i en undersøkelse i Rogaland i januar 2022 vist at 1 av 5 bedrifter har opplevd dataangrep eller hendelser knyttet til datasikkerhet siste 12 måneder [12], for bedrifter med flere enn 50 ansatte er tallet 35 %.

Risikoen for at informasjon kommer på avveie på grunn av at brukere ubevisst gjør feil er vurdert som høy fordi det er et stort antall aktører involvert, og all erfaring tilsier at den mest sårbare angrepsflaten er hver enkelt ansatt. Det er også arbeidshverdager preget av høyt tempo som gjør at man kan gjøre feil uten å vite det og/eller å mene det. Personopplysningers konfidensialitet kan også trues pga. brukernavn og passord til brukerkontoer med utvidede rettigheter (f.eks. administratorkonto) er på avveie internt i virksomheten. Dette er vurdert som høy risiko.

Det kan også være en risiko at personopplysninger sees av personer uten tjenstlig behov for eksempel pga. at den ansatte bruker en mobil løsning og ikke fysisk skjermer informasjonen slik at den blir sett av uvedkommende. Informasjonen er dermed kommet på avveie og kan misbrukes. Tilsvarende kan det være en risiko for at informasjon kommer på avveie pga. at ansatte bevisst bryter regler. Disse to hendelsene er vurdert til moderat risiko. Risikoen er vurdert som lav for at informasjon kommer på avveie til ansatte som ikke lenger har tjenstlig behov for informasjonen. Dette kan forekomme ved manglende eller forsinket vedlikehold av tilganger til ansatte som bytter stilling internt i samme virksomhet. Risikoen for at plattformen skal tilgjengeliggjøre informasjon til virksomheter som ikke skal ha, for eksempel på bakgrunn av teknisk feil ved oppdateringer eller andre hendelser vurderes som lav.

Identifisert risiko	Vurdert risiko
Informasjon på avveie på grunn av teknisk sårbarhet	
Informasjon på avveie på grunn av et tilfeldig eller målrettet angrep	
Informasjon på avveie fordi brukere ubevisst gjør feil	
Informasjonens konfidensialitet er truet på grunn av at brukernavn/passord for administrator/bruker med utvidede rettigheter til plattformen på avveie internt i virksomheten	
Informasjon på avveie gjennom at informasjonen er synlig og tilgjengelig for personer uten tjenstlig behov	
Informasjon på avveie fordi ansatte bevisst bryter regler	
Informasjon på avveie til ansatte som ikke lenger har tjenstlig behov for å se informasjonen	
Plattformen tilgjengeliggjør informasjon til virksomheter som ikke skal ha tilgang til informasjonen	

[12] 1 av 5 bedrifter rammet av dataangrep (nho.no)

4.2. Vurdering av identifiserte risikoer knyttet til integritet

Integritet handler om å sikre at informasjon er oppdatert, helhetlig og korrekt.

I vurderingen er det tre risikoer som utpeker seg som høye. Den ene er risiko for at ansatte skriver feil personopplysninger pga. feil eller uhell. Ansatte kan skrive inn eller endre data ved feil, uvitenhet eller slurv (eksempelvis dokumenterer på feil pasient). Vi har valgt å score denne risikoen høyt da plattformen og økosystemet vil håndtere en stor mengde aktører. Den andre risikoen handler om at ansatte ikke opplever at informasjon er oppdatert og pålitelig. En plattform skal stegvis realiseres. Det vil innebære en risiko for at informasjon ikke er oppdatert og pålitelig på alle områder, enten fordi ikke alle aktører er tilkoblet, eller at den stegvise utvikling ikke har omfattet det spesifikke området enda. I tillegg kan tilfeldige hendelser som f.eks. strømbrudd i infrastruktur i verdikjeden også føre til at informasjonen ikke oppleves som korrekt og pålitelig. Det blir veldig viktig å sikre at ansatte klarer å operere i et landskap der noe er oppdatert og følger nye rutiner, mens noe vil følge tidligere rutiner. I tillegg er risikoen for informasjonens integritet vurdert til høy pga. brukernavn/passord til brukerkontoer med utvidede rettigheter (f.eks. administratorkonto) er på avveie internt i virksomheten.

Det er vurdert til moderat risiko at ansatte kan skrive inn eller endre data med vilje. I tillegg er risikoen for informasjonens integritet vurdert til moderat pga. tilfeldige eller målrettede angrep.

I dag er det også enkelte sluttbrukerapplikasjoner der det kun er leverandører som kan endre eller slette informasjon. Dette ansees som en lav risiko, og vil først og fremst påvirke helsepersonellets tidsforbruk ved kontakt med leverandør dersom det må endres dokumentasjon i journalløsning eller annen applikasjon. Risikoen kan derfor foreligge for at det ikke blir gjort og at journalen vil inneholde feilinformasjon.

Identifisert risiko	Vurdert risiko
Informasjonens integritet kan være truet ved at ansatt skriver eller legger inn feil informasjon ved uhell	
Ansatt opplever at informasjonen ikke er korrekt og pålitelig ved tilfeldige hendelser som strømbrudd, serverkrasj osv	
Informasjonens integritet er truet på grunn av at brukernavn/passord for administrator/bruker med utvidede rettigheter til plattformen på avveie internt i virksomheten	
Informasjonens integritet kan være truet ved at ansatte bevisst skriver inn eller endrer informasjon	
Informasjonens integritet kan være truet grunnet at det gjennomføres tilfeldige eller målrettet angrep	
Informasjon blir ikke rettet eller slettet fordi det kun er leverandør som kan gjøre dette i sluttbrukerløsninger	

4.3. Vurdering av identifiserte risikoer knyttet til tilgjengelighet

Krav til tilgjengelighet handler om å sikre at informasjonen finnes der og når behovet oppstår.

En av de største risikoene identifisert på nåværende tidspunkt handler om utilgjengelig informasjon ved fullstendig bortfall av informasjon gjennom plattformen kort tid (under en dag) på bakgrunn av

tilfeldig eller målrettet angrep. Vi vurderer også risikoen som høy for at informasjon blir utilgjengelig pga. tilfeldige hendelser lenger enn en dag fra plattformen.

Det er vurdert til moderat risiko at ansatte opplever at sluttbrukerapplikasjoner er utilgjengelige. Felles risiko for alle er at det i en mellomperiode i en stegvis utvikling vil sammenstilles informasjon fra flere ulike kilder, og ved teknisk feil i eksempelvis integrasjoner, applikasjon, lokale servere eller plattform vil det være en større risiko for at en av kildene blir utilgjengelig. Bortfall av informasjon kan føre til utfordringer i å gi kritiske tjenester for å ivareta forsvarlig helsehjelp til innbyggere over kortere eller lengre perioder. Det er også vurdert til moderat risiko at ansatt kan oppleve å ikke ha informasjon tilgjengelig på grunn av fullstendig bortfall av plattformen (informasjon) kort tid (under en dag) på bakgrunn av tilfeldige hendelser. Tilsvarende at ansatt opplever å ikke ha informasjon tilgjengelig fra alle nødvendige kilder (også nasjonale løsninger) på bakgrunn av tilfeldig eller målrettede angrep. At ansatt opplever å ikke ha informasjon tilgjengelig pga fullstendig bortfall av plattformen (informasjon) over lang tid (over en dag) pga tilfeldige eller målrettede angrep er tilsvarende scoret moderat. Tilsvarende moderat risiko er satt knyttet til at informasjonens tilgjengelighet er truet pga brukernavn/passord for administrator/bruker med utvidede rettigheter til plattformen på avveie internt i virksomheten. Risiko vurderes som moderat for at informasjon ikke er tilgjengelig fordi ansatte ubevisst gjør feil.

At ansatte opplever å ikke ha informasjon tilgjengelig på grunn av fullstendig bortfall av plattformen (informasjon) over lang tid (over en dag) pga tilfeldige hendelser er scoret til lav. Risikoen for utilgjengelig informasjon presentert fra nasjonale felles løsninger over lang tid vurderes også som lav. Tilsvarende risiko vurderes også for at informasjon ikke er tilgjengelig fordi ansatte bevisst bryter regler eller ubevisst gjør feil.

Identifisert risiko	Vurdert risiko
Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) kort tid (under en dag) på bakgrunn av tilfeldig/målrettede angrep	
Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) over lang tid (over en dag) pga. tilfeldige hendelser	
Ansatt opplever at sluttbrukerapplikasjonene er utilgjengelige	
Ansatt opplever å ikke ha informasjon tilgjengelig fra alle nødvendige kilder på bakgrunn av tilfeldige hendelser	
Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) kort tid (under en dag) på bakgrunn av tilfeldige hendelser	
Ansatt opplever å ikke ha informasjon tilgjengelig fra alle nødvendige kilder (også nasjonale løsninger) på bakgrunn av tilfeldig eller målrettede angrep	
Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) over lang tid (over en dag) pga. tilfeldig/målrettede angrep	

Informasjonens tilgjengelighet er truet pga. brukernavn/passord for administrator/bruker med utvidede rettigheter til plattformen på avveie internt i virksomheten	
Ansatte opplever å ikke ha informasjon tilgjengelig fordi ansatte gjør feil	
Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) over lang tid (over en dag) pga. tilfeldige hendelser	
Ansatt opplever å ikke ha informasjon tilgjengelig fra nasjonale løsninger pga. tilfeldige hendelser	
Ansatte opplever å ikke ha informasjon tilgjengelig fordi ansatte bevisst bryter regler	

4.4. Vurdering av identifiserte risikoer knyttet til personvern/GDPR

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger[13]. Det vises til Bilag 5.1 for flere vurderinger knyttet til personvern.

Kommunene utfordres på å ivareta informasjonssikkerhet og personvern i eksisterende løsninger i dag. Den enkelte kommune kan ha 5-6 ulike journalløsninger som kommuniserer dårlig eller ikke i det hele tatt. Kommunene har krav etter §19 i pasientjournalloven å sørge for at relevante og nødvendige helseopplysninger er tilgjengelig for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelpen til den enkelte. Der man skulle delt informasjon direkte i løsningene må man i stedet kommunisere muntlig, per telefon, i møter, via e-meldinger eller på papir. Dette utfordrer informasjonssikkerhet og personvern, deriblant den enkelte registrertes muligheter til oversikt over behandlingen av egne opplysninger og utøve sine rettigheter.

Det foreligger også en risiko for at den registrerte ikke får ivaretatt sine rettigheter (ref. GDPR kap 3). Det vises til bilag 5.1 for ytterligere beskrivelse og vurdering av områdene[14] som hører inn under kap 3. En innbygger har etter pasient- og brukerrettighetsloven krav til å kunne utøve rett til journalinnsyn, retting/sletting og begrensning av innsyn etter §§5-1 til 5-3. Tilsvarende er det krevende for innbygger i dag å utøve rettighetene sine fordi informasjonen ligger lagret i ulike løsninger hos den enkelte behandler. Eksisterende løsninger i dag klarer heller ikke å overholde kravene på alle områder.

Kommunene er store virksomheter med mange ansatte, særlig innenfor helse- og omsorg. Kommunenes evne til å ivareta GDPR vurderes å ha en moderat risiko. Dette med bakgrunn i at kommunenes evne til å ivareta dette vil være varierende, og kreve kontinuerlig arbeid og ressurser eksempelvis i opplæring og bevisstgjøring av ansatte. Disse ansatte er blant annet helsepersonell som i årene som kommer vil oppleve enda høyere forventing til kapasitet og oppgaver.

En risiko som er identifisert, men som ansees som svært lav, er manglende hjemmel for behandling av personopplysninger. Majoriteten av tjenestene kommunene gir har hjemmel i lov, og resten er basert på samtykke.

[13] Personvern | Datatilsynet

[14] Retten til innsyn i egen informasjon, portabilitet, sletting, korrigering, protestering, begrensning

Med mange aktører og løsninger foreligger det en risiko for manglende og oppdatert oversikt over hvor ulike personopplysninger flyter mellom løsninger. Dette er helt sentralt å ha på plass og blir også en viktig del av videre arbeid med personvernvurderinger når det konkretiseres.

Identifisert risiko	Vurdert risiko
Virksomheten ivaretar ikke informasjonssikkerhet i tilstrekkelig grad (brudd på GDPR) på grunn av kompetansemangel	
Virksomheten har utfordringer med å ivareta informasjonssikkerhet og personvern i eksisterende løsninger i dag	
Virksomheten har utfordring med å ivareta den registreres rettigheter (GDPR kap 3)	
Virksomheten mangler hjemmel for behandling av personopplysninger	
Virksomheten mangler oversikt over flyt av personopplysninger i løsningen	

4.5. Vurdering av identifiserte risikoer knyttet til drift og forvaltning av IKT-funksjoner

Det er også gjort en overordnet vurdering av risiko spesifikt knyttet til drift og forvaltning av IKT-systemer og funksjoner, der tilgangsstyring er et viktig element. Det er grunnleggende viktig at tilgangsstyring, i likhet med alle andre sikkerhetsfunksjoner, etableres og sees i sammenheng i en helhetlig sikkerhetsarkitektur. Foruten tilgangsstyring[15], er også oversikt over enheter og programvare[16], konfigurasjonsstyring[17] og sikkerhetsovervåkning[18] viktige sikkerhetsfunksjoner som påvirker kapasitet og evne til beste praksis for tilgangsstyring.

Angripere forsøker ofte å få kontroll over legitime brukere og kontoer i IKT systemer. Neste mål er som regel å øke tilganger og rettighetsnivåer slik at kontoer kan utnyttes for å ta se lenger inn i systemet, samt få tilgang til flere ressurser

Kontroll med bruk av ulike funksjoner og tjenester ved tilgangsstyring er viktig. Tilgangsstyring må derfor sees på i sammenheng med alle funksjonene og tjenestene som skal ivareta tilgangsstyring, i seg selv, men også forsvarlig sikring av IKT-miljøene tilgangsstyrings funksjoner og tjenester utgjør del av.

Dagens situasjon og kompleksitet omfatter store teknologiske variasjoner og ulikheter. Det kan skape flere store og ressurskrevende utfordringer, særlig dersom man i plattformen skal forsøke å integrere og gjenbruke store deler av de eksisterende teknologiske løsningene som er etablert for tilgangsstyring i primærhelsetjenesten. Dette med hensyn til store teknologiske variasjoner og ulikhet, og grunnlag for høy kompleksitet i dagens ulike EPJ-løsninger.

15 Se for eksempel Grunnprinsipp 1.2 og Grunnprinsipp 2.6 i NSMs grunnprinsipper for IKT-sikkerhet

16 Se for eksempel grunnprinsipp 1.2 i NSMs grunnprinsipper for IKT-sikkerhet

17 Se for eksempel Grunnprinsipp 2.3 og Grunnprinsipp 2.10 i NSMs grunnprinsipper for IKT-sikkerhet

18 Se eksempelvis Grunnprinsipp 3.2 og Grunnprinsipp 3.3 i NSMs grunnprinsipper for IKT-sikkerhet.

Det er identifisert en risiko kategorisert som høy. Dette er en risiko som omfatter manglende oppdateringsregime for applikasjon, mobile enheter, operativsystemer, server, arbeidsstasjoner eller at registrerte eller kjente sårbarheter ikke rettes. Vi har vurdert denne risikoen til høy fordi det innenfor kommunale helse- og omsorgstjenester er mange aktører, og mange ulike versjoner av journalsystemene i drift. Aktørene kan ha utfordringer med å oppdatere journalsystemene eller andre systemer til enhver tid, eller leverandører kan ha utfordringer med kapasitet. Konsekvensene er særlig store dersom sårbarheter ikke rettes og dermed kan utgjøre en trussel for konfidensialitet, integritet og tilgjengelighet i hele økosystemet. På denne måten øker antallet tekniske sårbarheter og tilhørende angrepsvektorer[19] som kan utnyttes av angripere

Innenfor mer moderat risiko er det identifisert flere områder. Et av disse områdene handler om manglende forståelse av ansvar og utførelse av oppgaver mellom aktørene i økosystemet knyttet til kvalitet, oppetid/tilgjengelighet, funksjonalitet osv. Vi anser denne risikoen som moderat fordi vi tenker dette er et område det er reell påvirkningsmulighet på, for eksempel knyttet til å utarbeide gode avtaler mellom aktørene.

Det er også vurdert som en moderat risiko at brukernavn/passord for administratorrolle med utvidede rettigheter til plattformen kommer på avveie internt i virksomheten. Dette kan føre til at ansatte i eksempelvis drift og forvaltning av plattformen får uautorisert administrasjonstilgang til tjenesten/systemet.

Vi anser det også som en risiko dersom systemadministratorer eller annet lokalt IT-personell hos en av aktørene utfører uautoriserte endringer i løsninger som kan påvirke plattformen. Dette kan være særlig vesentlig i en mellomperiode, i en stegvis utvikling. Vi har mange lokale databaser og løsninger i de enkelte kommunene eller hos andre aktører som fastleger der endringer vil kunne påvirke samhandlingsevnen med plattformen.

En annen risiko som er vurdert som moderat er manglende tilgangsstyring på grunn av manglende forståelse av egen rolle, ansvar og oppgaver i økosystemet med mange ulike aktører.

Identifisert risiko	Vurdert risiko
Målrettet/tilfeldig angrep på grunn av at sårbarheter i systemer ikke rettes/patches pga. manglende rutine eller oppdateringsregime	
Målrettet/tilfeldig angrep pga. sårbarheter oppstår fordi sentrale oppgaver og ansvar ikke ivaretas pga. manglende forståelse av ansvar og utførelse av oppgaver mellom aktørene i økosystemet	
Systemadministrator eller annet lokalt IT personell i primærhelsetjenesten eller andre aktører utfører uautoriserte endringer i løsninger som påvirker plattformen (verdikjedeproblematikk)	
Manglende tilgangsstyring på grunn av manglende forståelse av oppgaver, roller og ansvar som fører til at autorisasjon og autentisering ikke blir forvaltet korrekt	

[19] Metoden en angriper velger for å utføre et angrep på en datamaskin, et nettverk eller et system. Eksempler på angrepsvektorer er e-postvedlegg, websider, chat og sosial manipulering.

5. EVALUERING AV RISIKO

Det tredje steget i risikovurderingen er evaluering av risiko. Formålet er å gi støtte til beslutninger om hvilke risikoer som må håndteres, og hvilken prioritet håndteringen av dem bør gis. Det går ut på å sammenligne risikonivået som ble avdekket i analysen av risiko i steget foran, med kriterier for å akseptere risiko. Dette er kriterier ledelsen må beslutte og gi som føringer for arbeidet på et senere tidspunkt.

I denne overordnede risikovurderingen kommer vi med eksempler på aktuelle tiltak for å redusere risikonivået og anbefaler at de identifiserte hendelsene med kritisk/høy risiko får høyest prioritet. Deretter må de identifiserte hendelsene med moderat risiko prioriteres.

5.1. Eksempel på tiltak for hendelser med kritisk/høy risiko

Område	Identifisert risiko	Eksempler på tiltak
Konfidensialitet	Informasjon (personopplysninger) på avveie på grunn av teknisk feil	• Bruk av rammeverket NSMs grunnprinsipper for IKT-sikkerhet for å metodisk sikre informasjonssystemene i økosystemet (applikasjoner, IKT-plattformer samt digital og fysisk IKT-infrastruktur). Bruk i tillegg produsent- og teknologispesifikk beste praksis, for sikre forsvarlig bruk av enkeltteknologier. • Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Foreslå sikkerhetstiltak for de ulike delene av løsningene som eksisterer i de enkelte løsningene i dag (f.eks. kryptering, brannmur og fysisk/logisk sikkerhet for å ha et akseptabelt risikonivå) • Definer enhetlige sikkerhetspolicyer for behandling av persondata • Definer krav til høy sikkerhet for løsningene som må være oppfylt hos aktørene som er leverandører i økosystemet • Rutiner som beskriver ansvarsforhold og hva som skal gjøres når personopplysninger/virksomhetskritiske opplysninger kommer på avveie • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy)

		• Dedikerte ressurser som har overvåkning og analyser av sikkerhet som hovedoppgave • Automatiserte logg analyser • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • God opplæring av ansatte og jevnlig informasjon
Konfidensialitet	Informasjon på avveie på grunn av et tilfeldig eller målrettet angrep	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Sentralisert IAM (Identity and Access Management) løsning • Felles rutiner og retningslinjer for rollebasert tilgangsstyring • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Dedikerte ressurser som har overvåkning og analyser av sikkerhet som hovedoppgave • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • God opplæring av ansatte og jevnlig informasjon
Konfidensialitet	Informasjon på avveie fordi brukere ubevisst gjør feil	• God opplæring av ansatte og jevnlig informasjon • Automatiserte logg analyser • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Jevnlige varslede og ikke-varslede øvelser
Konfidensialitet	Informasjonens konfidensialitet er truet på grunn av at brukernavn/passord for administrator/bruker med utvidede rettigheter til	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy)

	plattformen på avveie internt i virksomheten	• Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • Rutiner for at ledere må jevnlig/månedlig kontrollere at aktive tilganger for sine ansatte stemmer og sørge for å fjerne tilganger til ansatte som har sluttet • God opplæring av ansatte og jevnlig informasjon
Integritet	Informasjonens integritet er truet på grunn av at brukernavn/passord for administrator/bruker med utvidede rettigheter til plattformen på avveie internt i virksomheten	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • Rutiner for at ledere må jevnlig/månedlig kontrollere at aktive tilganger for sine ansatte stemmer og sørge for å fjerne tilganger til ansatte som har sluttet • God opplæring av ansatte
Integritet	Informasjonens integritet kan være truet ved at ansatt skriver eller legger inn feil informasjon ved uhell	• God prosess-støtte i applikasjonene for å unngå at blant annet dokumentasjon skrives på feil pasient • God opplæring av ansatte og jevnlig informasjon
Integritet	Ansatt opplever at informasjonen ikke er korrekt og pålitelig ved tilfeldige hendelser som strømbrudd, serverkrasj osv.	• God opplæring av ansatte og jevnlig informasjon • Sørge for at rutiner og informasjon til enhver tid er oppdatert i forhold til stegvis utvikling • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt

Tilgjengelighet	Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) kort tid (under en dag) på bakgrunn av tilfeldig/målrettede angrep	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Redusert kompleksitet og angrepsflater ved å forenkle IKT-driftsmiljø(er) • Sentralisert IAM (Identity and Access Management) løsning • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Dedikerte ressurser som har overvåkning og analyser av sikkerhet som hovedoppgave • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger
Tilgjengelighet	Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) over lang tid (over en dag) pga. tilfeldige hendelser	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Redusert kompleksitet og angrepsflater ved å forenkle IKT-driftsmiljø(er) • Sentralisert IAM (Identity and Access Management) løsning • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Dedikerte ressurser som har overvåkning og analyser av sikkerhet som hovedoppgave • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger
Drift/forvaltning	Målrettet/tilfeldig angrep på grunn av at sårbarheter i systemer ikke rettes/patches pga. manglende rutine	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Redusert kompleksitet og angrepsflater ved å forenkle IKT-driftsmiljø(er) • Sentralisert IAM (Identity and Access Management) løsning

	eller oppdateringsregime	• Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Dedikerte ressurser som har overvåkning og analyser av sikkerhet som hovedoppgave • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger. Sørge for at policy/rutiner/informasjon om hvilke versjoner som lokal IT må forholde seg til er oppdatert og sendes ut til aktuelle IT miljø • God opplæring av ansatte og jevnlig informasjon

5.2. Eksempel på tiltak for hendelser med moderat risiko

Område	Identifisert risiko	Eksempler på tiltak
Konfidensialitet	Informasjon på avveie gjennom at informasjonen er synlig og tilgjengelig for personer uten tjenstlig behov	• Rutiner for bruk av mobile løsninger • Rutiner som beskriver ansvarsforhold og hva som skal gjøres når personopplysninger/virksomhetskritiske opplysninger kommer på avveie • God opplæring av ansatte
Konfidensialitet	Informasjon på avveie fordi ansatte bevisst bryter regler	• Sikkerhetsfunksjoner sentraliseres • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Automatiserte logg analyser • Konsekvenser ved brudd på retningslinjer • God opplæring av ansatte
Integritet	Informasjonens integritet kan være truet ved at ansatte bevisst skriver inn eller endrer informasjon	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Automatiserte logg analyser

		• Konsekvenser ved brudd på retningslinjer • God opplæring av ansatte
Integritet	Informasjonens integritet kan være truet grunnet at det gjennomføres tilfeldige eller målrettet angrep	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Redusert kompleksitet og angrepsflater ved å forenkle IKT-driftsmiljø(er) • Sentralisert IAM (Identity and Access Management) løsning • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Dedikerte ressurser som har overvåkning og analyser av sikkerhet som hovedoppgave • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • God opplæring av ansatte
Tilgjengelighet	Ansatt opplever at sluttbrukerapplikasjonene er utilgjengelige	• Systemovervåkning • Rutiner med tydelige roller, oppgaver og ansvar også inkludert leverandører av sluttbruker applikasjonene
Tilgjengelighet	Ansatt opplever å ikke ha informasjon tilgjengelig fra alle nødvendige kilder på bakgrunn av tilfeldige hendelser	• Systemovervåkning • Varsler om at informasjon ikke er tilgjengelig fra aktuell kilde i sluttbruker applikasjoner
Tilgjengelighet	Ansatt opplever å ikke ha informasjon tilgjengelig fra alle nødvendige kilder (også nasjonale løsninger) på bakgrunn av tilfeldig eller målrettede angrep	• Systemovervåkning • Varsler om at informasjon ikke er tilgjengelig fra aktuell kilde i sluttbruker applikasjoner
Tilgjengelighet	Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) over lang tid (over en dag) pga.	• Systemovervåkning • Varsler om at informasjon ikke er tilgjengelig fra aktuell kilde i sluttbruker applikasjoner • Sentrale drifts tjenester og ressurser med riktig kompetanse

	tilfeldig/målrettede angrep	• Sørge for at alle virksomheter i økosystemet har beredskapsplaner for bortfall av tjeneste og/eller data • Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Redusert kompleksitet og angrepsflater ved å forenkle IKT-driftsmiljø(er) • Sentralisert IAM (Identity and Access Management) løsning • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Dedikerte ressurser som har overvåkning og analyser av sikkerhet som hovedoppgave • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • God opplæring av ansatte
Tilgjengelighet	Informasjonens tilgjengelighet er truet pga. brukernavn/passord for administrator/bruker med utvidede rettigheter til plattformen på avveie internt i virksomheten	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • Rutiner for at ledere må jevnlig/månedlig kontrollere at aktive tilganger for sine ansatte stemmer og sørge for å fjerne tilganger til ansatte som har sluttet • God opplæring av ansatte
Tilgjengelighet	Ansatte opplever å ikke ha informasjon tilgjengelig fordi ansatte gjør feil	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy)

		• Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • Rutiner for at ledere må jevnlig/månedlig kontrollere at aktive tilganger for sine ansatte stemmer og sørge for å fjerne tilganger til ansatte som har sluttet • God opplæring av ansatte
Personvern (GDPR)	Virksomheten ivaretar ikke informasjonssikkerhet i tilstrekkelig grad (brudd på GDPR) på grunn av kompetansemangel	• Kontinuerlig opplæring og bevisstgjøring av medarbeidere i personvern og informasjonssikkerhet • Rutiner
Personvern (GDPR)	Virksomheten har utfordringer med å ivareta informasjonssikkerhet og personvern i eksisterende løsninger i dag	• Sentralisering av sikkerhetsfunksjoner • Sentralisering av datalagring • Sørge for at nødvendig informasjon om den enkelte pasient er tilgjengelig og oppdatert på tvers av systemer i virksomheten • Sørge for at alle journalsystemer har tilgangslogg
Personvern (GDPR)	Virksomheten har utfordring med å ivareta den registreres rettigheter (GDPR kap 3)	• Sentralisering av sikkerhetsfunksjoner • Sentralisering av datalagring • Sørge for at innbygger får innsyn i egne personopplysninger • Sørge at innbygger kan utføre sin rett til å få opplysninger om seg selv korrigert og slettet
Drift/forvaltning	Brukernavn/passord for administrator/bruker med utvidede rettigheter til plattformen på avveie	• Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • Rutiner for at ledere må jevnlig/månedlig kontrollere at aktive tilganger for sine

		ansatte stemmer og sørge for å fjerne tilganger til ansatte som har sluttet • God opplæring av ansatte
Drift/forvaltning	Målrettet/tilfeldig angrep pga. sårbarheter oppstår fordi sentrale oppgaver og ansvar ikke ivaretas pga. manglende forståelse av ansvar og utførelse av oppgaver mellom aktørene i økosystemet	• HUKI matrise for ansvarsforhold mellom kommuner/fastleger/aktører, plattformforvalter, nasjonale aktører • Rutiner og retningslinjer hvis ansvarsforholdene i HUKI matrisen ikke ivaretas • Sikkerhetsfunksjoner sentraliseres i henhold til anbefalinger i beste praksis for IKT-sikkerhet • Redusert kompleksitet og angrepsflater ved å forenkle IKT-driftsmiljø(er) • Sentralisert IAM (Identity and Access Management) løsning • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Dedikerte ressurser som har overvåkning og analyser av sikkerhet som hovedoppgave • Felles rutiner for hvordan sikkerhetshendelser skal håndteres sentralt og lokalt • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • God opplæring av ansatte
Drift/forvaltning	Systemadministrator eller annet lokalt IT personell i primærhelsetjenesten eller andre aktører utfører uautoriserte endringer i løsninger som påvirker plattformen (verdikjedeproblematikk)	• Rutiner og retningslinjer angående ansvar og rolle forståelse • Oppdatert informasjon om systemiske avhengigheter • Sikkerhetsfunksjoner sentraliseres • Sentralisert IAM (Identity and Access Management) løsning • Felles rutiner og retningslinjer for rollebasert tilgangsstyring • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • God opplæring av ansatte
Drift/forvaltning	Manglende tilgangsstyring på grunn	• Sikre god dokumentasjon, god overføring av kompetanse og kunnskap i virksomhetene

	av manglende forståelse av oppgaver, roller og ansvar som fører til at autorisasjon og autentisering ikke blir forvaltet korrekt	• Ressurser dedikert til dette område og oppfølging • Rutiner og retningslinjer angående ansvar, rolle og oppgave forståelse • Oppdatert informasjon om systemiske avhengigheter • Sikkerhetsfunksjoner sentraliseres • Sentralisert IAM (Identity and Access Management) løsning • Felles rutiner og retningslinjer for rollebasert tilgangsstyring • Sentrale systemer for overvåking og analyser av sikkerhet (f.eks. SIEM verktøy) • Automatiserte logg analyser • Rutiner for gjennomgang av logger med mistenkelige tilganger • God opplæring av ansatte

6. VIDERE ARBEID MED RISIKO

I forbindelse med planlegging og gjennomføring av utprøvingsfase må prosjektet og tilhørende deltagere gjennomføre tiltak for å sørge for akseptabel risiko. Det må også gjennomføres konkrete risiko- og sårbarhetsvurderinger for hver utprøvning.

Det må lages en plan med tydelige frister og hvem som er ansvarlig for gjennomføringen. Planen skal forankres hos prosjektets ledelse. Dersom et planlagte tekniske tiltak for å oppnå akseptabel risiko ikke kan innføres umiddelbart, bør risikoreduserende administrative tiltak i form av f.eks. rutine vurderes. Risikomatrisen etter tiltak er gjennomført må oppdateres.

7. UNDERLAG

7.1. Risiko- og sårbarhetsanalyse

Risiko- og Sårbarhetsanalyse

Formål

For å sikre god innretning av arbeid med informasjonssikkerhet og personvern er det gjennomført en overordnet risikovurdering i forhold til en tenkt første kommune som tar i bruk tiltaket. I denne fasen har vi ikke detaljkunnskap om løsningselementene (plattform, understøttende IKT-infrastruktur samt applikasjonene som skal kjøres mot plattformen). Det medfører at overordnede betraktninger og vurderinger legges til grunn i vurderingen. Dette er gjort med bakgrunn i å etablere et grunnlag for kunnskap om verdier som behandles i og av økosystemet.
Risikovurderingen kan gi grunnlag for både ny og samlet kunnskap om forutsetninger og prinsipper som kan bli gjeldende. Den kan også legges til grunn for å planlegge tilpassede risikoreduserende tiltak, eksempelvis i arbeid med utprøving, design- og utvikling, anskaffelser og implementering. I forbindelse med utprøving kan denne risikovurderingen brukes som grunnlag for arbeidet med informasjonssikkerhet og personvern. For å klassifisere hendelsene er rapport fra prosjektet Felles nasjonalt klassifikasjonssystem for uønskede hendelser brukt

Id	Område	Klassifisering/Årsak	Uønskede hendelser	Beskrivelse	Konsekvens for hvem eller hva	Eksisterende tiltak	Sannsynlighet	Konsekvens	Risikoverdi
1	Konfidensialitet	3.4.6/ Svikt i IKT	Informasjon på avveie på grunn av teknisk sårbarhet	Dette kan skje av ulike årsaker, og mange integrasjoner øker risiko. Noen eksempler er manglende kryptering av data "in transit (SSL/TLS)» over offentlige nettverk gjør det mulig for andre å avlytte datatrafikk, hacking, eller teknisk feil hos en av aktørene som gjør at informasjon kommer på avveie	Brudd på lov (GDPR) for virksomhet Økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger på avveie for den registrerte	Sikkerhet i løsningene (kryptering, brannmur og det som ligger rundt løsningene i dag)	3	4	12

2	Konfidensialitet	2.5.9/ Menneskelig svikt	Informasjon på avveie gjennom at informasjonen er synlig og tilgjengelig for personer uten tjenstlig behov	Eksempelvis kan mobile løsninger medføre en risiko for at informasjon sees av personer uten tjenstlig behov der den ansatte befinner seg. Evt hjemmekontor. Denne informasjonen kan dermed komme på avveie eller misbrukes.	Brudd på lov (GDPR) for virksomhet Økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger på avveie for den registrerte	Rutiner/ prosedyrer	2	4	8
3	Konfidensialitet	2.5.9/ Menneskelig svikt	Informasjon på avveie fordi brukere ubevisst gjør feil	Ansatte kan ubevisst gjøre feil og tilgjengeliggjøre informasjon ved bruk av digitale verktøy, mobile verktøy	Brudd på lov (GDPR) for virksomhet Økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger på avveie for den registrerte		4	4	16
4	Konfidensialitet	3.1.4/ Prosedyre ikke fulgt	Informasjon på avveie til ansatte som ikke lenger har tjenstlig behov for å se informasjonen	For eksempel ved manglende vedlikehold av tilgang og tilgangsstyring, ved bytte av arbeidsted innad i virksomheten etc. Manglende periodisk revisjon og kontroll av roller, rettigheter og ansvar til tjenesten/ systemet/ løsningen. Særlig relevant for ansatte som bytter arbeidssted, men internt i samme virksomhet slik at man fortsatt har AD tilgang.	Brudd på lov (GDPR) for virksomhet Økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger på avveie for den registrerte	Rutiner/ prosedyrer	2	2	4
5	Konfidensialitet	2.5.9/ Menneskelig svikt	Informasjon på avveie fordi ansatte bevisst bryter regler	Ansatte kan snoke eller hente ut data for å misbruke. Dette kan være av egen vinning, eller på grunn av press eller økonomiske fordeler	Brudd på lov (GDPR) for virksomhet Økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger på avveie for den registrerte	Retningslinjer	2	4	8

6	Konfidensialitet	3.4.6/ Svikt i IKT	Plattformen tilgjengeliggjør informasjon til virksomheter som ikke skal ha tilgang til informasjonen	For eksempel grunnet teknisk feil ved oppdateringer eller andre hendelser	Brudd på lov (GDPR) for virksomhet Store økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger på avveie for den registrerte		1	4	4
7	Konfidensialitet	3.4.6/ Svikt i IKT	Informasjon på avveie på grunn av et tilfeldig eller målrettet angrep	Et tilfeldig angrep kan skyldes skadevare som eksempelvis kryptovirus, løsevare Målrettet angrep eksempelvis fra hackere. Kan gjøres på grunn av egen vinning, cyberkriminalitet, egen underholdning Målrettede angrep kan være hacking gjennomført på oppdrag fra aktører	Brudd på lov (GDPR) for virksomhet Store økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger på avveie for den registrerte Svikt i helse og omsorgstjenester med fare for liv og helse	Sikkerhet i løsningene (kryptering, brannmur og det som ligger rundt løsningene i dag)	4	4	16
8	Konfidensialitet	3.1.4/ Prosedyre ikke fulgt	Informasjonens konfidensialitet er truet på grunn av at brukernavn/passord for administrator/bruker med utvidede rettigheter til plattformen kommer på avveie internt i virksomheten	Ansatte i forvaltning og drift av plattform får uautorisert administratortilgang til tjenesten/systemet og dette utfordrer konfidensialiteten	Brudd på lov (GDPR) for virksomhet Store økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger på avveie for den registrerte Svikt i helse og omsorgstjenester med fare for liv og helse	Rutiner/ prosedyrer	2	5	10
9	Integritet	2.5.9/ Prosedyre ikke fulgt	Informasjon blir ikke rettet eller slettet fordi det kun er leverandør som kan gjøre dette i sluttbrukerløsninger	Hvis de skal endre dokumentasjon i journalløsning eller annen applikasjon må de kontakte leverandør for bistand til dette. I enkelte sluttbrukerapplikasjoner er det	Brudd på lov (GDPR) for virksomhet Personopplysninger for den registrerte er ikke korrekte	Rutiner/ prosedyrer	1	2	2

				kun leverandør som kan endre eller slette informasjon					
10	Integritet	2.5.9/ Menneskelig svikt	Informasjonens integritet kan være truet ved at ansatte bevisst skriver inn eller endrer informasjon	Ansatte kan skrive inn eller endre data som ikke skal være der, pga vond vilje	Brudd på lov (GDPR) for virksomhet Økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger om den registrerte er ikke korrekte	Retningslinjer	2	4	8
11	Integritet	2.5.9/ Menneskelig svikt	Informasjonens integritet kan være truet ved at ansatt skriver eller legger inn feil informasjon ved uhell	Ansatte kan skrive inn eller endre data som ikke skal være der, både pga ansatte som gjør feil uvitende, uhell, slurv (dokumenterer på feil pasient)	Brudd på lov (GDPR) for virksomhet Økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger om den registrerte er ikke korrekte		4	4	16
12	Integritet	3.4.6/ Svikt i IKT	Informasjonens integritet kan være truet grunnet at det gjennomføres tilfeldige eller målrettet angrep	Ved tilfeldige angrep kan informeres endres, slettes etc	Brudd på lov (GDPR) for virksomhet Store økonomiske tap (eks. bøter) for virksomhet Tap av omdømme for virksomhet (ved konsekvens for innbyggere) Personopplysninger om den registrerte er ikke korrekte	Sikkerhet i løsningene (kryptering, brannmur og det som ligger rundt løsningene i dag)	2	4	8
13	Integritet	3.4.1/ Svikt i IKT	Ansatt opplever at informasjonen ikke er korrekt og pålitelig ved tilfeldige hendelser som strømbrudd, serverkrasj osv	Pga ulike hendelser er ikke oppdatert informasjon som er tilgjengelig i løsningen	Brudd på lov (GDPR) Økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Fare for liv og helse for den registrerte		4	4	16

14	Integritet	3.1.4/ Prosedyre ikke fulgt	Informasjonens integritet er truet på grunn av at brukernavn/passord for administrator/bruker med utvidede rettigheter til plattformen på avveie internt i virksomheten	Ansatte i forvaltning og drift av plattform får uautorisert administratortilgang til tjenesten/systemet og kan utfordre informasjonens integritet.	Brudd på lov (GDPR) Økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Personopplysninger om den registrerte er ikke korrekt	Rutiner/ prosedyrer	2	5	10
15	Tilgjengelighet	3.4.1/ Svikt i IKT	Ansatt opplever at sluttbrukerapplikasjonene er utilgjengelige	Ansatte vil ikke ha tilgang til informasjon. Kan medføre bortfall av kritiske tjenester for å ivareta forsvarlig helsehjelp til innbyggere over lengre tid.	Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Fare for liv og helse for den registrerte	Gjennomføre ROS analyse ved ibruktagelse av løsninger. Beredskapsplaner ved hendelser. Tydelig rolle og oppgave ansvar, også opp mot leverandør.	2	4	8
16	Tilgjengelighet	3.4.1/ Svikt i IKT	Ansatt opplever å ikke ha informasjon tilgjengelig fra alle nødvendige kilder på bakgrunn av tilfeldige hendelser	I en stegvis utvikling vil økosystemet bestå av mange ulike løsninger og lagringsmuligheter (lokale kopier, sluttbrukerløsninger som lagrer, plattformen nede). Informasjon vil i en mellomperiode være tilgjengelig fra flere ulike kilder. Grunnet feil i integrasjoner, eller applikasjon, lokale servere og plattform) kan det være en risiko for det er kilder som kan være utilgjengelige.	Brudd på lov (GDPR)		2	4	8
17	Tilgjengelighet	3.4.1/ Svikt i IKT	Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) kort tid	Ansatte får ikke tilgang til relevant informasjon til sitt arbeid i en periode på under en dag	Brudd på lov (GDPR) Økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Fare for liv og helse for den registrerte	Rutiner/ prosedyrer	2	4	8

			(under en dag) på bakgrunn av tilfeldige hendelser						
18	Tilgjengelighet	3.4.1/ Svikt i IKT	Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) over lang tid (over en dag) pga tilfeldige hendelser	Ansatte får ikke tilgang til relevant informasjon til sitt arbeid på mer enn en dag	Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Fare for liv og helse for den registrerte	Rutiner/ prosedyrer	2	5	10
19	Tilgjengelighet	3.4.1/ Svikt i IKT	Ansatt opplever å ikke ha informasjon tilgjengelig fra nasjonale løsninger pga. tilfeldige hendelser	Nasjonale løsninger er utilgjengelige. Plattformens egenskap i å sammenstille informasjon vil derfor ikke fungere	Brudd på lov (GDPR)	Rutiner/ prosedyrer	1	4	4
20	Tilgjengelighet	2.5.9/ Menneskelig svikt	Ansatte opplever å ikke ha informasjon tilgjengelig fordi ansatte bevisst bryter regler	Ansatte kan bevisst flytte pasienter organisatorisk eller på andre måter blokkere andres ansatte tilgang til relevant informasjon	Brudd på lov (GDPR) Fare for liv og helse for den registrerte	Retningslinjer	1	4	4
21	Tilgjengelighet	2.5.9/ Menneskelig svikt	Ansatte opplever å ikke ha informasjon tilgjengelig fordi ansatte gjør feil	Ansatte kan ubevisst flytte pasienter organisatorisk eller på andre måter blokkere andres ansatte tilgang til relevant informasjon	Brudd på lov (GDPR) Fare for liv og helse for den registrerte		2	4	8
22	Tilgjengelighet	3.4.1/ Svikt i IKT	Ansatt opplever å ikke ha informasjon tilgjengelig fra alle nødvendige kilder (også nasjonale løsninger) på bakgrunn av tilfeldig eller målrettede angrep		Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Fare for liv og helse for den registrerte	Sikkerhet i løsningene (kryptering, brannmur og det som ligger rundt løsningene i dag)	3	3	9

23	Tilgjengelighet	3.4.1/ Svikt i IKT	Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) kort tid (under en dag) på bakgrunn av tilfeldig/målrettede angrep		Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Fare for liv og helse for den registrerte	Sikkerhet i løsningene (kryptering, brannmur og det som ligger rundt løsningene i dag)	3	4	12
24	Tilgjengelighet	3.4.1/ Svikt i IKT	Ansatt opplever å ikke ha informasjon tilgjengelig pga. fullstendig bortfall av plattformen (informasjon) over lang tid (over en dag) pga. tilfeldig/målrettede angrep		Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Fare for liv og helse for den registrerte	Sikkerhet i løsningene (kryptering, brannmur og det som ligger rundt løsningene i dag)	1	5	5
25	Tilgjengelighet	3.1.4/ Prosedyre ikke fulgt	Informasjonens tilgjengelighet er truet pga. brukernavn/passord for administrator/bruker med utvidede rettigheter til plattformen på avveie internt i virksomheten	Ansatte i forvaltning og drift av plattform får uautorisert administratortilgang til tjenesten/systemet og kan ta ned hele tjenesten. Dette kan utfordre tilgjengelighet	Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Fare for liv og helse	Rutiner/ prosedyrer	1	5	5
26	Personvern (GDPR)	2.5.9/ Prosedyre ikke fulgt	Virksomheten mangler hjemmel for behandling av personopplysninger		Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Ulovlig behandling av den registrertes personopplysninger	Rutiner/ prosedyrer	1	4	4

27	Personvern (GDPR)	2.5.9/ Prosedyre ikke fulgt	Virksomheten mangler oversikt over flyt av personopplysninger i løsningen	Manglende skisse over dataflyt	Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere)	Rutiner/ prosedyrer	1	3	3
28	Personvern (GDPR)	2.5.9/ Prosedyre ikke fulgt	Virksomheten ivaretar ikke informasjonssikkerhet i tilstrekkelig grad (brudd på GDPR) på grunn av kompetansemangel	Manglende gjennomføring av kontinuerlig opplæring og bevisstgjøring av medarbeidere i personvern og informasjonssikkerhet	Brudd på lov Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Registrertes rettigheter blir ikke ivaretatt	Obligatorisk opplæring i informasjonssikkerhet og personvern for nytilsatte	2	3	6
29	Personvern (GDPR)	2.5.9/ Prosedyre ikke fulgt	Virksomheten har utfordringer med å ivareta informasjonssikkerhet og personvern i eksisterende løsninger i dag		Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Registrertes rettigheter blir ikke ivaretatt	Gjennomføre DPIA for hver ny løsning som tas i bruk, samt oppdatere vurderingen etter anbefalte retningslinjer	3	3	9
30	Personvern (GDPR)	2.5.9/ Prosedyre ikke fulgt	Virksomheten har utfordring med å ivareta den registreres rettigheter (GDPR kap 3)	Den registrerte får ikke oppfylt: Retten til innsyn i egne opplysninger, retten til portabilitet, retten til sletting, retten til korrigering, retten på å protestere, retten til begrensing	Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Registrertes rettigheter blir ikke ivaretatt	Rutiner/ prosedyrer	2	3	6
31	Drift/ forvaltning	3.4.1/ Svikt i IKT	Målrettet/tilfeldig angrep på grunn av at sårbarheter i systemer ikke rettes/patches pga. manglende rutine eller oppdateringsregime	Kommuner, fastleger og andre relevante aktører i økosystemet. Manglende oppdateringregime for applikasjon/ webapp/ app for mobil enhet, operativsystem, server, arbeidsstasjon og oppdagede/kjente sårbarheter rettes/patches ikke	Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Fare for liv og helse for den registrerte	Rutiner/ prosedyrer	3	4	12

32	Drift/ forvaltning	3.5.6/ Uklare ansvarsforhold	Målretta/tilfeldig angrep pga. sårbarheter oppstår fordi sentrale oppgaver og ansvar ikke ivaretas pga. manglende forståelse av ansvar og utførelse av oppgaver mellom aktørene i økosystemet	Dette kan gjelde eksempelvis knyttet til kvalitet, oppetid/tilgjengelighet, funksjonalitet osv	Brudd på lov (GDPR) Store økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Fare for liv og helse for den registrerte	Rutiner/ prosedyrer	2	4	8
33	Drift/ forvaltning	3.4.1/ Svikt i IKT	Systemadministrator eller annet lokalt IT personell i primærhelsetjenesten eller andre aktører utfører uautoriserte endringer i løsninger som påvirker plattformen (verdikjedeproblematikk)	Spesielt vesentlig i mellomperiode (Stegvis utvikling). Vi har mange lokale databaser, og der kan systemadm og annet IT-personell i primærhelsetjenesten gjøre uautoriserte endringer som kan påvirke plattformen	Økonomiske konsekvenser Fare for liv og helse ved bortfall av informasjon Tap av omdømme	Rutiner/ prosedyrer	2	4	8
34	Drift/ forvaltning	3.5.6/ Uklare ansvarsforhold	Manglende tilgangsstyring på grunn av manglende forståelse av oppgaver, roller og ansvar som fører til at autorisasjon og autentisering ikke blir forvaltet korrekt	Manglende forståelse av egen rolle, ansvar og oppgave i økosystemet med mange ulike aktører	Brudd på lov (GDPR) Økonomiske tap (eks. bøter) Tap av omdømme (ved konsekvens for innbyggere) Registrertes personopplysninger kan	Rutiner/ prosedyrer	2	3	6

7.2. Definisjoner i Risiko- og sårbarhetsanalyse

Risikoverdi = sannsynlighet * konsekvens

Risikoverdien vil være et tall mellom 1 og 25. Vi opererer med følgende tolkning av risikoverdien:

Lav risiko:	≤	Risikoverdi	≤	4		
Moderat risiko:	≤	Risikoverdi	≤	9		terskel for tiltak
Høy risiko:	≤	Risikoverdi	≤	16		
Kritisk risiko:	≤	Risikoverdi	≤	25		

Hvis konsekvensen av en risikofaktor er vurdert som kritisk, så vil risikoverdien aldri bli under ”moderat” selv om sannsynligheten for at risikofaktoren skal inntreffe er vurdert som ”lav”. Dette gjenspeiler behovet for at prosjekter alltid må følge opp risikofaktorer med potensielt kritiske konsekvenser og revurdere disse med jevne mellomrom, for å sikre at sannsynligheten for at de inntreffer ikke har økt.

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

Sannsynlighet	Lite sannsynlig	Noe sannsynlig	Sannsynlig	Ganske sannsynlig	Meget sannsynlig
-	Fra en gang pr år til hvert 10 år	1-4 ganger pr år	1 gang i mnd	Ukentlig	Daglig

Konsekvens	Ubetydelig	Mindre alvorlig	Betydelig	Alvorlig	Svært alvorlig
Liv og helse	Ubetydelig, ingen skader på personer eller ansattes arbeidssituasjon.	Mindre skader på personer eller ansattes arbeidssituasjon. Medfører ikke sykefravær.	Flere syke og/eller alvorlig personskade, innleggelse på sykehus, langvarig sykefravær. Betydelig skade på de ansattes arbeidssituasjon.	Enkeltdødsfall og/eller stor smittespredning. Stor skade på ansattes arbeidssituasjon.	Flere døde. Ugjenopprettelig skade på de ansattes arbeidssituasjon.
Tilgjengelighet/ operativ evne	Tjeneste blir ikke påvirket. Ubetydelig påvirkning.	Bortfall av tjeneste/leveranse innenfor operative mål (serviceerklæring, avtaler o.l.) i enkeltområder. Mindre driftsforstyrrelser som fører til små endringer i tjenesteproduksjon.	Bortfall av tjeneste utover operative mål (timer) i enkeltområder. Driftsforstyrrelser som medfører omfattende endringer i tjenesteproduksjon.	Bortfall av tjeneste utover operative mål (dager i enkeltområder eller timer i større områder). Kommunen kan kun levere begrenset med lovpålagte tjenester.	Langvarig svikt som rammer større områder utover flere dager. Kommunen evner ikke å levere lovpålagte tjenester.
Omdømme / tillit	Ingen omtale eller innvirkning.	Noe negativ omtale hos medier og interessenter.	Negativ omtale hos medier og interessenter som svekker tilliten til oss.	Betydelig negativ omtale hos medier og interessenter, som stiller spørsmål ved vår evne til å løse vårt samfunnsoppdrag.	Massiv omdømmeskade og uopprettelig tillitssvikt rammer vår ledelse og/eller styre.
Ytre miljø	Ingen miljøskader. Ubetydelig restitusjonstid.	Kortvarig lokal påvirkning av lukt, støy og begrenset utslipp til jord, vann og luft. Kort restitusjonstid etter påført miljøkonsekvenser.	Påvirkning på ytre miljø med omfattende utslipp til jord, vann og luft. Lang restitusjonstid etter påført miljøkonsekvenser.	Langvarig skader på flora og fauna. Fiskedød, omfattende utslipp til vann/jord.	Alvorlig utslipp med irreversibel effekt og varig miljøkonsekvens. Fare for liv og helse.
Materiell/ økonomi	Skaden(e) har en kostnad på under 10 000 kroner.	Skaden(e) har en kostnad på mellom 10 000 og 100 000 kroner.	Skaden(e) har en kostnad på mellom 100 000 og 1 000 000 kroner.	Skaden(e) har en kostnad på mellom 1 000 000 og 5 000 000 kroner, eller virksomheten har mer enn 1 uke på å skaffe til veie likvide midler over 500 000 kroner.	Skaden(e) har en kostnad på over 5 000 000 kroner, eller virksomheten har under 1 uke på å skaffe til veie likvide midler over 1 000 000.

Konfidensialitet	Intet uautorisert innsyn i helse- og personopplysninger, ikke brudd på personvernet	Uautorisert innsyn i enkelte helse- og personopplysninger og lovbrudd, Brudd på personvernet for et lite antall pasienter	Uautorisert innsyn i flere helse- og personopplysninger, mulighet for endring og brudd på lov, Brudd på personvernet for et moderat antall pasienter	Uautorisert innsyn i store mengder helse- og personopplysninger, mulighet for endring og brudd på lov, Brudd på personvernet for et stort antall pasienter	Fullt uautorisert innsyn i eller mulighet for endring av alle helse- og personopplysninger og brudd på lov, Tilgang til behandlingsrettet helseregister (inkl. EPJ) og helse- og personopplysninger kommer på avveie
Integritet	Mangel på integritet vil være ubetydelig, neglisjerbar.	Mangel på integritet er mindre viktig, men kan påvirke internt arbeid (data går tapt).	Mangel på integritet kan skape merarbeid for å verifisere korrekthet og/eller tap av tillit hos enkeltaktører og/eller mindre grupper av aktører (mistanke om endring).	Mangel på integritet kan skape store mengder merarbeid for å verifisere korrekthet og/eller tap av tillit som påvirker evnen til å utføre en funksjon, eller gjøre det vanskelig å gjenskape korrekt data (data på avveie).	Mangel på integritet kan skape store mengder merarbeid for å verifisere korrekthet og/eller tap av tillit som påvirker evnen til å utføre en funksjon, eller gjøre det umulig å gjenskape korrekt data (data er korrupt, endret, modifisert, lagt til, eller byttet ut).