NORMEN

Veileder om risikostyring for informasjonssikkerhet og personvern

Versjon 1.1

21. november 2022

Utarbeidet med støtte fra Direktoratet for e-helse

Vedtatt av Styringsgruppen for Normen

Denne veilederen er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Normen forvaltes av Styringsgruppen for Normen, etter Normens forvaltningsmodell.

Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt. Innbyggere og ansatte skal være trygge på at opplysninger om dem behandles på en sikker måte i helse- og omsorgssektoren. Normen skal bidra til å at virksomheter i helse- og omsorgssektoren kan ha gjensidig tillit til hverandre, ved å etablere mekanismer og regler som sørger for at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Alt om Normen, Normens krav og veiledningsmateriell finnes på www.normen.no.

En til enhver tid oppdatert versjon av veilederen finnes på www.normen.no. Dersom du har spørsmål knyttet til veilederen kan du sende spørsmål og kommentarer til: sikkerhetsnormen@ehelse.no

Innhold

1 Innledning

1.1 Bakgrunn

Nåværende versjon av Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) har økt fokus på risikostyring utover selve risikovurderingen, sammenlignet med tidligere versjoner av Normen.

Helse- og omsorgsdepartementet har også gjennom rundskriv av 2019 gitt oppmerksomhet til temaet, og klargjort en del problemstillinger knyttet til informasjonshåndtering, pasientsikkerhet, personvern og informasjonssikkerhet.

Normens veiledningsmateriell for ulike aktiviteter som inngår i risikostyringen i helse- og omsorgssektoren har vært fordelt på en rekke ulike faktaark, som

- Faktaark 04 – Kartlegge og klassifisere systemer
- Faktaark 05 – Fastsette nivå for akseptabel risiko
- Faktaark 07 – Risikovurdering

Implementeringen av personvernforordningen tydeliggjorde kravet til vurdering av personvernkonsekvenser, som gjorde det naturlig for Normen å også knytte dette temaet nærmere de andre aktivitetene.

På bakgrunn av denne utviklingen har det vært behov for å oppdatere veiledningsmateriellet på risikoområdet for å sette de ulike risikorelaterte aktivitetene inn i en større sammenheng, i en egen veileder om risikostyring for helse- og omsorgssektoren.

1.2 Tema for veilederen

Denne veilederen skal gi veiledning til, og bidra til etterlevelse av, kravene i Normen knyttet til risikostyring.

Risikostyring beskrives i Normens kapittel 3 som koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko.

Det omfatter å få oversikt over informasjon og teknologi i virksomheten, identifisere trusler og mulige uønskede hendelser for både virksomheten og de registrerte, analysere risikoen og etablere tiltak for å opprettholde ~~nivå for~~ akseptabel risiko.

Veilederen gjengir Normens krav overordnet i kapittel 1.4 Krav i Normen, mens nærmere utdypning av kravene og hvordan de kan løses i praksis følger i kapittel 2 Risikostyring i helse- og omsorgssektoren.

1.3 Målgruppe

Målgruppen for veilederen er virksomheter som omfattes av Normen og som skal sikre etterlevelse av Normens krav, herunder dataansvarlig.

Veilederen er nyttig for alle ledere og medarbeidere i helse- og omsorgssektoren med en rolle innenfor risikostyringen, eller som har behov for å forstå hvordan risiko styres og

håndteres i egen sektor eller virksomhet. Lederansvaret får særlig fokus i kapittelet om roller og ansvar, men ledere i helse- og omsorgssektoren er en særlig viktig målgruppe for veilederen som helhet. Kapittelet om risikovurdering vil være særlig relevant for medarbeidere som skal delta i en risikovurdering. De som skal lede risikovurderingsprosesser i virksomheten bør lese hele veilederen.

Veilederen kan også være nyttig for systemleverandører og andre samarbeidspartnere til helse- og omsorgssektoren, som på grunn av sin leveranse eller engasjement er omfattet av Normen 6.0 gjennom avtale med virksomheten eller Norsk Helsenett SF. Særlig gjelder dette der databehandlere eller andre skal bidra til risikovurderinger eller andre deler av dataansvarliges risikostyring.

1.4 Krav i Normen

Denne veilederen tar i all hovedsak for seg kravene i Normens kapittel 3. Risikostyring. Øvrige krav som berøres inkluderer krav om roller og ansvar i kapittel 2. Ledelse og ansvar.

Tabellen som følger, gir en oversikt over sentrale krav for risikostyring fra Normen. Merk at tabellen ikke er uttømmende for en virksomhets totale risikostyring, og at mer om hvordan kravene i tabellen kan løses i praksis følger i kapittel 2 Risikostyring i helse- og omsorgssektoren.

Virksomheten er ansvarlig for å	Se mer om kravet i Normen
Sørge for at virksomheten følger gjeldende krav til informasjonssikkerhet og personvern, og at virksomhetens informasjonsbehandling gir et sikkerhetsnivå som er egnet med hensyn til risikoen og behandlingens art. Dette inkluderer å sette føringer for vurdering og håndtering av risiko, herunder fastsette kriterier for å akseptere risiko, samt å sørge for velfungerende styring og kontroll. Dette ansvaret ligger hos virksomhetens øverste ledelse.	Kapittel 2. Ledelse og ansvar; Kapittel 2.2 Dataansvarliges ansvar
Bistå dataansvarlig med personvern og informasjonssikkerhet slik at egnet sikkerhetsnivå blir ivaretatt i de tilfeller der virksomheten er databehandler.	Kapittel 2. Databehandlers ansvar
Etablere koordinerte aktiviteter for å rettlede og kontrollere virksomheten med hensyn til risiko (risikostyring).	Kapittel 3. Risikostyring
Etablere forholdsmessige tekniske og organisatoriske tiltak.	Kapittel 3.1 Forholdsmessighet ved valg av tiltak
Sørge for at virksomhetens behandlinger har et egnet sikkerhetsnivå i tråd med Normens minimumskrav til informasjonssikkerhet og eventuelt egne informasjonssikkerhetsmål	Kapittel 3.2 Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet

Ha oversikt over teknologi og behandling av helseopplysninger, inkludert • protokoll over behandlinger av helse- og personopplysninger, og • oversikt over IKT-systemer, infrastruktur, digitale tjenester og annen informasjon med betydning for informasjonssikkerheten, mv.	3.3 Oversikt over teknologi og behandling av helse- og personopplysninger
Vurdere og håndtere risiko, med utgangspunkt i kartlegging av informasjonsverdier og hva som vil bli konsekvensen av hendelser som rammer tilgjengeligheten, integriteten og konfidensialiteten til informasjonsverdiene. Virksomheten skal vurdere sannsynligheten for og mulige konsekvenser av at en hendelse inntreffer. Dersom risikoen er uakseptabel, skal virksomheten gjennomføre tiltak for å redusere risikoen.	Kapittel 3.4 Risikovurdering og risikohåndtering
Vurdere hvilke konsekvenser behandling av helse- og personopplysninger medfører for den registrerte. Hvis det er sannsynlig at en behandling medfører høy risiko for de registrerte, skal virksomheten gjennomføre en mer grundig personvernkonsekvens-vurdering, også kalt DPIA.	Kapittel 3.5 Vurdering av personvernkonsekvenser; Kapittel 3.5.1 Personvernkonsekvensvurdering

1.5 Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk

Forskrift for ledelse og kvalitetsforbedring i helse- og omsorgstjenesten skal bidra til faglig forsvarlige helse- og omsorgstjenester, kvalitetsforbedring og pasient- og brukersikkerhet, og at øvrige krav i helse- og omsorgslovgivningen etterleves. Dette skal blant annet gjøres ved å etablere internkontroll og arbeide systematisk, og særlig § 5-6 er relevante for kravene som ligger til grunn for denne veilederen. De beskriver henholdsvis at man skal tilpasse styringssystemet sitt etter blant annet risikoforhold; og at man skal ha oversikt over områder med risiko i virksomheten og hvordan man kan minimalisere denne.[1]

Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) beskriver virksomheters plikter ved behandling av helseopplysninger, og § 22 fremhever at dataansvarlige og databehandleren skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, og viser til personvernforordningens artikkel 32.[2]

Det er flere artikler fra Lov om behandling av personopplysninger (personopplysningsloven) som er relevante for kravene som dekkes av denne veilederen. Loven gjennomfører

[1] Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten: https://lovdata.no/dokument/LTI/forskrift/2016-10-28-1250
[2] Lov om behandling av helseopplysninger ved ytelse av helsehjelp, 2014: https://lovdata.no/dokument/NL/lov/2014-06-20-42

personvernforordningen (GDPR) i Norge. Forordningens artikkel 24 beskriver dataansvarliges ansvar, og beskriver at virksomheten skal gjennomføre egnede tekniske og organisatoriske tiltak basert på risiko for fysiske personers rettigheter og friheter.[3]

Det samme fremheves i forordningens artikkel 32, som fremhever at virksomheten skal ta hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad, for å gjennomføre egnede tekniske og organisatoriske tiltak. Videre beskrives at ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til omstendighetene og risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.[4]

Se for øvrig vedlegget til Normen, med samlet oversikt over alle Normens krav og lovhjemmel for disse, på Normens nettsider.[5]

I tillegg til Normens krav, som er grunnlaget for Normens veiledning, baseres metoden for risikovurdering blant annet på elementer fra NS 5814 – Krav til risikovurderinger fra Norsk Standard. Standarden ble første gang utgitt i 2008 og den nyeste utgaven kom i mai 2021. Standarden har innlemmet aktiviteter, begreper og kvaliteter fra to andre risikostandarder, NS 5832 og NS-ISO 31000, for å vise risikovurderingenes plass i den overordnede risikostyringen.[6]

Videre ser denne veilederen hen til Digitaliseringsdirektoratets veiledningsmateriell innen internkontroll og risikostyring, som Internkontroll i praksis – informasjonssikkerhet[7] samt sentrale krav og aktiviteter som beskrives i Digitaliseringsdirektoratets sammenstilling av standarden ISO/IEC 27001:2013 tilpasset norsk offentlig sektor.[8] Det samme gjelder Veiledning i helhetlig styring og kontroll av informasjonssikkerhet, som er resultatet av et samarbeid mellom Nasjonal sikkerhetsmyndighet, Direktoratet for forvaltning og økonomistyring og Digitaliseringsdirektoratet, med bidrag fra Datatilsynet og KS.[9]

1.6 Avgrensninger

Denne veilederen er avgrenset til risikostyring innenfor Normens temaområder i helse- og omsorgssektoren. Det er i all hovedsak kravene i Normens kapittel 3. Risikostyring som behandles i denne veilederen. Øvrige krav som berøres inkluderer krav om roller og ansvar i kapittel 2. Ledelse og ansvar.

---

[3] Lov om behandling av personopplysninger, 2018: https://lovdata.no/dokument/NL/lov/2018-06-15-38/
[4] Lov om behandling av personopplysninger, 2018: https://lovdata.no/dokument/NL/lov/2018-06-15-38/
[5] Normens nettsider, Oversikt over Normens krav, https://www.ehelse.no/normen/oversikt-over-normens-krav-og-mapping-mellom-iso-og-normen
[6] Norsk Standard, NS5814 – Krav til risikovurderinger, 2021: https://www.standard.no/fagomrader/kvalitet-og-/risikostyring/ns-5814-krav-til-risikovurderinger/
[7] Digitaliseringsdirektoratet, Internkontroll i praksis – informasjonssikkerhet, https://www.digdir.no/informasjonssikkerhet/internkontroll-i-praksis-informasjonssikkerhet/2601
[8] Digitaliseringsdirektoratet, Hva sier ISO/IEC 27001?, https://www.digdir.no/informasjonssikkerhet/kva-seier-ns-isoiec-27001/3060
[9] Digitaliseringsdirektoratets nettsider, Helhetlig styring og kontroll av informasjonssikkerhet, https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284

Når anbefalingene i veilederen tas i bruk i virksomheten, må de tilpasses med utgangspunkt i virksomhetens kompleksitet og størrelse, samt konkrete behov og oppgaver. Det kan være ulike måter å etterleve enkeltkrav på.

Selv om risikostyring er en prosess som er en del av en virksomhets helhetlige internkontroll tar ikke denne veilederen for seg øvrige krav som er en del av internkontrollen. Disse beskrives i Veileder om internkontroll, som ble utviklet parallell med denne veilederen. Det vil være nyttig å lese særlig kapittel 2.1 om roller og ansvar i internkontrollveilederen, for å sørge for en god forståelse av disse prosessene.

2 Risikostyring i helse- og omsorgssektoren

I helse- og omsorgssektoren handler risiko i ytterste konsekvens om liv og død. For å yte helsehjelp og levere forsvarlige helse- og omsorgstjenester må risiko håndteres på tvers av ulike fagområder som informasjonssikkerhet, personvern og pasientsikkerhet. Disse områdene er imidlertid tett knyttet, og bidrar sammen til forsvarlige helse- og omsorgstjenester for pasienter og brukere.

Gode helsetjenester forutsetter at relevante pasientopplysninger kan deles. God pasientsikkerhet krever at opplysninger lagres og deles mellom helsepersonell, at opplysningene er korrekte og oppdaterte, samt at pasient/bruker og helsepersonell har tillit til systemer og personell. Mangelfull informasjon og svikt i overganger innad og mellom helsetjenestenivåer er dokumentert som et av de største risikoområdene for god pasientsikkerhet.[10]

Informasjonssikkerhet handler om å håndtere risiko relatert til informasjon og behandling av personopplysninger. Informasjonens integritet, tilgjengelighet og konfidensialitet skal sikres. Systemer og organisasjoner som behandler informasjonen må være robuste. Det vil si at de må ha en tilstrekkelig evne til å gjenopprette normaltilstand etter en uønsket hendelse.[11] Informasjonssikkerhet er ikke et formål i seg selv, men har som formål å støtte opp under virksomhetens andre formål. God informasjonssikkerhet er viktig for å kunne levere forsvarlige helsetjenester.

Videre skal vi sikre pasienter og brukeres personvern, ved å behandle de registrertes helse- og personopplysninger etter personvernprinsippene.[12] Slik oppfyller vi deres rettigheter etter personvernforordningen. Pasient- og brukerperspektivet er viktig i arbeidet med risiko, informasjonssikkerhet og personvern. Ulike pasienter eller pasientgrupper kan ha ulike behov og forventninger, og det vil ofte være nyttig å være i dialog med disse for å søke å ivareta deres interesser på best mulig måte.

---

[10] Helse- og omsorgsdepartementet, Rundskriv I-3/2019 om informasjonshåndtering i spesialisthelsetjenesten, 2019: https://www.regjeringen.no/no/dokumenter/rundskriv-i-32019-om-informasjonshandtering-i-spesialisthelsetjenesten/id2642049/

[11] Integritet, tilgjengelighet, konfidensialitet og robusthet er definert i Normens kapittel 1.0.

[12] Se Normens faktaark 57 om personvernprinsippene, https://www.ehelse.no/normen/faktaark/faktaaark-57-personvernprinsippene

Normen foreskriver at virksomhetene, innenfor lovverkets rammer, skal søke en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet. Risikostyring er blant de viktigste verktøyene for å søke en slik balansert tilnærming, inkludert risikovurderinger av informasjonssikkerhet og vurderinger av personvernkonsekvenser.

En sentral del av risikostyringen i sektoren handler med andre ord om å veie ulike viktige hensyn opp mot hverandre og avgjøre hvilken risiko virksomheten kan akseptere både totalt sett og i enkeltprosesser. Dette beskrives blant annet i Helse- og omsorgsdepartementets rundskriv om informasjonshåndtering fra 2019.[13]

Vi må ha disse perspektivene med oss i ulike deler av den helhetlige risikostyringen, samt før, under og etter at man har gjennomført en risikovurdering.

2.1 Roller og ansvar

Virksomhetene i helse- og omsorgssektoren er dataansvarlig for all behandling av helse- og personopplysning som skjer i eller på vegne av virksomheten. Dataansvarlig er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. Ansvaret skal ivaretas av den daglige ledelsen av virksomheten.

Det er ledelsen som har ansvaret for risikostyringen, og for å beslutte hvilken risiko virksomheten aksepterer. Dette gjelder uavhengig av hvorvidt risikoen befinner seg på informasjonssikkerhets-, personvern-, pasientsikkerhetsområdet eller andre relevante områder. Virksomhetens organisering må understøtte dette ansvaret, og sørge for gode prosesser som gir beslutningsgrunnlag av tilstrekkelig kvalitet i den helhetlige risikostyringen.

Virksomheter som benytter databehandlere, for eksempel leverandører av systemer for elektronisk pasientjournal, må sørge for at dette blir en integrert del av den overordnede risikostyringen. Databehandler er noen som behandler personopplysninger på vegne av den dataansvarlige. Det presiseres at en databehandler er en ekstern person eller virksomhet utenfor den dataansvarliges virksomhet. Den dataansvarlige må sørge for (og avtalefeste gjennom databehandleravtalen) at helse- og personopplysninger behandles i henhold til akseptabel risiko i alle ledd av verdikjeden, også hos eventuelle underleverandører.

Den følgende tabellen beskriver ulike roller i risikostyringen, med tilhørende beskrivelse og eksempler.

Rolle	Beskrivelse
Virksomhetens leder	Ansvarlig for risikostyringen som helhet. Beslutter hvilken risiko virksomheten aksepterer.
Risikoeier	Definert av virksomheten som ansvarlig for måloppnåelse og tilhørende risiko på et definert område etter forhåndsdefinerte kriterier. For særlig høy risiko vil risikoeier ofte være virksomhetens leder.

[13] Helse- og omsorgsdepartementet, Rundskriv I-3/2019 om informasjonshåndtering i spesialisthelsetjenesten, 2019: https://www.regjeringen.no/no/dokumenter/rundskriv-i-32019-om-informasjonshandtering-i-spesialisthelsetjenesten/id2642049/

Systemeier	Sørger for at sitt informasjonssystem tilfredsstiller Normens krav, inkludert med hensyn til risiko.
Nøkkelpersoner	I denne veilederen beskrives nøkkelpersoner som deltar i risikovurderinger og/eller vurderinger av personvernkonsekvenser som brukere av systemer og opplysninger (blant annet helsepersonell), jurister, informasjonssikkerhetspersonell, IKT-personell fra relevante fagområder (f.eks. server, nettverk), personvernrådgivere, og databehandlere/leverandører. Bidrar med relevant fagkompetanse.
Personvernombud	Ledelsens rådgiver på personvernområdet. Gir råd i forbindelse med gjennomføring av personvernkonsekvensvurderinger (DPIA).
Alle medarbeidere	Følge virksomhetens prosedyrer og være bevisst på risiko i egne arbeidsoppgaver.

Hvordan ulike roller og tilhørende ansvar opptrer i de ulike delprosessene som inngår i risikostyringen beskrives i de ulike kapitlene av denne veilederen.

For å få en bedre forståelse av hvordan roller og ansvar innen risikostyring forholder seg til de øvrige rollene og ansvaret i internkontrollen bør du også lese delkapittel 2.1 om roller og ansvar i Normens Veileder om internkontroll i helse- og omsorgssektoren.

2.2 Oversikt over teknologi og behandling av helse- og personopplysninger

Ved å etablere og vedlikeholde oversikt over helse- og personopplysningene som behandles, og teknologi som brukes, kan virksomheten identifisere potensielle risikoområder den bør være spesielt oppmerksom på.

Virksomheten skal ha oversikt over:

- behandlinger av helse- og personopplysninger, ofte kalt behandlingsprotokoll eller behandlingsoversikt; og
- IKT-systemer, infrastruktur, digitale tjenester og annen informasjon med betydning for informasjonssikkerheten, mv.

Disse vil være viktige underlagsdokumenter for risikostyringen og de ulike risikovurderingene som skal gjennomføres i virksomheten.

2.2.1 Behandlingsprotokoll

Alle virksomheter som behandler helse- og personopplysninger skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar. Den samme plikten gjelder virksomhetenes databehandlere.

Du finner detaljert informasjons om behandlingsprotokollen og hva denne skal inneholde i Faktaark 13 – Protokoll over behandlinger av helse- og personopplysninger i virksomheten.[14]

Når man skal gjennomføre en risikovurdering eller en personvernkonsekvensvurdering (DPIA) bør man alltid først konsultere behandlingsprotokollen. Der kan du finne dokumentasjon om behandlingen av helse- og personopplysninger som kan danne grunnlag for videre vurdering av risiko.

Dersom du skal gjennomføre en risikovurdering og ikke finner behandlingen beskrevet i protokollen, bør du benytte anledningen til å føre den opp i protokollen. Ofte vil en risikovurdering og oppføring i protokollen til en viss grad skje i parallell. Oppstart av en risikovurdering er også en god anledning til å oppdatere protokollen med ny informasjon som fremkommer gjennom vurderingen.

Noen virksomheter velger å også inkludere enkle betraktninger knyttet til risiko ved de ulike behandlingene i sin behandlingsprotokoll, eller lenke til relaterte risikovurderinger som kan være nyttige.

2.2.2 Oversikt over systemer og teknologi

Virksomhetens leder er ansvarlig for å kartlegge og klassifisere alle systemer og teknologi som benyttes til behandling av helse- og personopplysninger i virksomheten. I praksis er typisk oppgaven delegert til avdelingsledere / systemeiere.

Formålet er å kjenne til hvilke systemer og teknologi som er kritiske for at virksomheten kan yte sine tjenester og å kunne prioritere de ulike systemene i henhold til kritikalitet. Dette vil også være nyttig vurderinger for å kunne prioritere i en beredskapssituasjon. Oversikten skal omfatte alle systemer som inneholder helse- og personopplysninger i tillegg til registre/systemer i elektromedisinsk utstyr og grunnleggende infrastruktur, som virksomheten benytter eller er avhengig av for å yte sine tjenester.

Kritikaliteten til de ulike systemene skal primært vurderes med hensyn til tilgjengelighet (hvor kritiske ikke-planlagte stopp vil være for det å kunne levere helse- og omsorgstjenester), men vil også kunne påvirkes av forhold tilknyttet integritet. Dersom det er tilfelle, bør dette også dokumenteres i oversikten. De kritiske systemene må være robuste, og ha tilstrekkelig evne til å gjenopprette normaltilstand etter en uønsket hendelse. Det er viktig å ta hensyn til avhengigheter i vurderingene, slik at systemer som i seg selv ikke er kritiske, kan få en høyere kritikalitet fordi de inngår som komponent i en større sammenheng.

Vedlegg 3.1 viser eksempler på hvordan ulike typer virksomheter kan prioritere sine systemer.

Virksomhetens kartlegging bør resultere i en dokumentert og prioritert oversikt over systemer og teknologi (inkludert IKT-systemer, infrastruktur, digitale tjenester og annen informasjon med betydning for informasjonssikkerheten, mv.). Kartlegging og klassifisering av systemer i

[14] Normen, Faktaark 13 - Protokoll over behandlinger av helse - og personopplysninger i virksomheten v3.0, 2018: https://www.ehelse.no/normen/faktaark/faktaark-13-protokoll-over-behandlinger-av-helse-og-personopplysninger-i-virksomheten

henhold til kritikalitet skal dokumenteres før behandling av helse- og personopplysninger starter.

Eksempel:
Normvik legesenter har tatt den årlige sikkerhetspraten – de har gjennomført ledelsens gjennomgang. Et av funnene fra gjennomgangen er at legesenteret ikke har satt opp en oversikt over systemer og teknologi, med tilhørende prioritering. Det vil da være utfordrende å jobbe med risikostyring for de ulike systemene.

Legesenteret går derfor gjennom sine systemer og vurderer hvor kritiske de ulike systemene er for at de skal klare å yte forsvarlig helsehjelp. De vurderer blant annet at laboratoriesystemer med særskilt viktige funksjoner som blodtype må ha aller høyeste prioritet, da de vil være kritiske for å yte forsvarlig helsehjelp.

Tabellen som følger viser hvordan Normvik legesenter prioriterte noen av sine systemer, med tilhørende beskrivelse av kritikaliteten. Merk at vurdering og prioritering her bare er et eksempel, og at virksomheten må vurdere dette basert på egne konkrete behov (med hensyn til konfidensialitet, integritet, tilgjengelighet og robusthet).

System	Prioritet	
Laboratoriesystem med særskilt viktige funksjoner	1	Systemer hvor stopp av tjeneste er eller kan være livstruende for bruker/pasient inklusive feilmedisinering, eller kritisk for virksomhetens drift
Elektronisk pasientjournal (EPJ)	1	Systemer hvor stopp av tjeneste er eller kan være livstruende for bruker/pasient inklusive feilmedisinering, eller kritisk for virksomhetens drift
Øvrige laboratoriesystem	2	Systemer hvor stopp av tjeneste kan få alvorlige konsekvenser, f.eks. medføre - tapt tillit hos bruker - betydelig merarbeid for personell - tapt effektivitet
Pasientadministrativt system (PAS)	2	Systemer hvor stopp av tjeneste kan få alvorlige konsekvenser, f.eks. medføre - tapt tillit hos bruker - betydelig merarbeid for personell - tapt effektivitet

2.2.3 Akseptabel risiko

Med akseptabel risiko menes i Normen hvor stor risiko virksomheten kan akseptere for at det inntreffer en hendelse som kan forårsake brudd på kravene til konfidensialitet, integritet og tilgjengelighet/robusthet i et konkret tilfelle. Litt enkelt sagt skal akseptabel risiko beskrive hvor hyppige hendelser med en viss alvorlighetsgrad virksomheten kan akseptere på et område uten at det påvirker tjenesteleveransen eller at virksomheten påføres uakseptable kostnader.

Det er dataansvarlig som har ansvar for at virksomhetens informasjonssystemer har egnet sikkerhetsnivå. Med egnet sikkerhetsnivå menes i Normen at sikkerhetstiltakene er tilpasset behandlingens egenart og gir en akseptabel restrisiko. Hver enkelt virksomhet må vurdere

konkret hvordan egnet sikkerhetsnivå og akseptabel risiko for vedkommende virksomhet skal oppnås.

Arbeidet med å fastsette akseptabel risiko skal gjøres med utgangspunkt i de enkelte behandlingene av helse- og personopplysninger virksomheten gjør. Disse finner du i behandlingsprotokollen. Det er også hensiktsmessig å bygge videre på prioriteringen som er gjort i forbindelse med utarbeidelse av oversikten over systemer og teknologi. Den vil være nyttig for å si noe om hvilken tilgjengelighet de ulike systemene krever.

Det finnes flere måter å jobbe med akseptabel risiko på. Metodene vektlegger ulike aspekter – noen definerer nivåer for akseptabel risiko og benytter disse til å styre risikoen, mens andre benytter definerte akseptkriterier for å oppnå samme utfall. Disse metodene kan også brukes i kombinasjon med hverandre.

Akseptkriterier for risiko kan benyttes for å kunne sammenligne/vekte risiko, slik at risiko kan prioriteres for håndtering. Slike kriterier kan videre bidra til at det gjøres gode valg i balansegangen mellom å etablere sikringstiltak, akseptere risiko og å la være å gjøre aktiviteter som innebærer for høy risiko.

Et nyttig utgangspunkt for utarbeidelsen av slike kriterier kan være minimumskravene til informasjonssikkerhet som er definert i Normens kapittel 3.2 «Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet». Disse kan være en rettesnor hvordan man tenker om hvilke risikoer som må eskaleres oppover i ledelsen, og som eventuelt ikke kan aksepteres.

Hvilken risiko som kan aksepteres vil variere etter omstendighetene, blant annet hvor stor betydning aktiviteten har for pasientbehandlingen, risikoens alvorlighet for den enkelte og rettferdighetsbetraktninger (som at nytte og risiko treffer ulike personer). Ved valg av egnede tekniske og organisatoriske tiltak skal virksomheten vurdere tiltakene opp mot virksomheten, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv. Virksomheten skal sørge for at det er forholdsmessighet mellom risiko og tiltakets kostnad.

Aksept av høyere risiko krever bedre ledelsesforankring. Det er hensiktsmessig for virksomheten å forhåndsdefinere hvilken risiko som kan aksepteres på ulike nivåer i virksomheten og hvem som eier risikoen. For svært høy risiko er det trolig kun virksomhetens øverste leder/ledelse som skal kunne akseptere den.

Vedlegg 3.4 viser et eksempel på hvordan man kan strukturere hvem som kan akseptere risiko etter hvilke kriterier.

Eksempel:
Normveien Psykologpraksis har gjennomført en oppdatering av risikovurderingen av sitt pasient-administrative system (PAS), og ser at et av scenarioene fra risikovurderingen nå befinner seg i den røde delen av risikomatrisen – det har høy risiko. Risikovurderingen er gjennomført av en liten arbeidsgruppe bestående av tre psykologer og praksisens helsesekretær, som er superbruker av systemet.

En av de tre psykologene har ledet arbeidsgruppen, og han er usikker på hvordan en høy risiko skal håndteres. Han går derfor til praksisens styringssystem, der metodikken for risikovurdering er beskrevet sammen med prosesser for den øvrige risikostyringen. Der finner han praksisens akseptkriterier.

Akseptkriteriene beskriver følgende:

Risikonivå	Kriterier for å akseptere risiko
Høy	Det er gjennomført et systematisk og svært grundig arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak.
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av daglig leder i Normveien Psykologpraksis. Aksept skal begrunnes og dokumenteres.

Det blir klart for psykologen at han og arbeidsgruppen må bidra til å identifisere eventuelle alternative arbeidsmåter og risikoreduserende tiltak, samt et grunnlag for å vurdere nytteverdien av PAS opp mot risikoen i scenarioet, før daglig leder eventuelt vurderer å akseptere risikoen. Han setter i gang med dette arbeidet.

Merk at vurderingene i dette eksempelet kun er for å illustrere metodikken. Virksomheten må selv etablere og vurdere i henhold til egne akseptkriterier.

Dersom man ønsker å utarbeide av nivåer for akseptabel risiko kan man ta utgangspunkt i en skala for konsekvens og sannsynlighet (se Vedlegg 3.2 og 3.3 for eksempler). Denne skalaen benyttes for å beskrive risikonivået, og som skal aksepteres i henhold til akseptkriterier eller fastsatte risikonivåer. Ved å sammenligne resultatet fra en risikovurdering med nivået man har satt for akseptabel risiko, vil man kunne vurdere om aktiviteten kan gjennomføres innenfor akseptabelt risikonivå. For all risiko som er høyere enn nivå for akseptabel risiko skal det iverksettes tiltak for å bringe risiko innenfor et akseptabelt nivå.

Vedlegg 3.2 viser et eksempel på en skala for ulike sannsynlighetsnivåer fremstilt som både frekvens og tiltaksstyrke. Vedlegg 3.2 viser et eksempel på en skala for ulike konsekvensnivåer og hva disse kan være innen tilgjengelighet, konfidensialitet og integritet.

Eksempel:
Etter at de gjennomførte en prioritering av systemene sine og fastsatte akseptabelt risikonivå for de ulike systemene i henhold til kommunens rutiner, gjennomfører Normvik legesenter en risikovurdering av et laboratoriesystem.

Et av scenarioene de vurderer gir en risiko på gult nivå basert på legesenterets skalaer for sannsynlighet og konsekvens. Nivå for akseptabel risiko for dette scenarioet er på grønt nivå. Dette er illustrert i legesenterets risikomatrise som følger:

	5 Svært sannsynlig					
Sannsynlighet	4 Sannsynlig					
	3 Mulig					
	2 Mindre sannsynlig		Akseptabel risiko		Risiko i scenarioet	
	1 Usannsynlig					
Risikomatrise		1 Ubetydelig	2 Lav	3 Moderat	4 Alvorlig	5 Svært alvorlig
		Konsekvens				

På grunnlag av dette beslutter legesenteret å gjennomføre tiltak for å bringe risikoen ned på et akseptabelt nivå. Merk at vurderingene i dette eksempelet kun er for å illustrere metodikken. Virksomheten må selv vurdere i henhold til egne behov og skalaer.

2.3 Risikovurdering

Alle virksomheter i helse- og omsorgssektoren skal gjennomføre risikovurderinger. Risikovurderingene skal være tilpasset virksomhetens størrelse og omfanget av behandling av helse- og personopplysninger. Risikovurderinger skal gjennomføres før behandling av helse- og personopplysninger startes, og ved endringer av behandlinger som kan påvirke sikkerheten.

Slike tilfeller kan for eksempel være:

- etablering av eller endring i behandling av helse- og personopplysninger eller annen informasjon av betydning for informasjonssikkerheten
- etablering av nye systemer eller registre som inneholder eller benytter helse- og personopplysninger eller annen informasjon av betydning for informasjonssikkerheten
- etablering av organisatoriske, tekniske eller andre endringer med betydning for informasjonssikkerheten
- etablering eller endring tilgang til helseopplysninger mellom virksomheter

I tillegg bør virksomhetens ledelse jevnlig gjennomføre risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten.

Dataansvarlig er ansvarlig for at det gjennomføres risikovurdering av behandlingen av helse- og personopplysninger. Risikovurderinger dokumenterer at dataansvarlig har iverksatt tilstrekkelige tiltak og at behandlingene utføres innenfor nivå for akseptabel risiko.

Virksomhetene er pålagt å vurdere sannsynlighet for og konsekvens av sikkerhetsbrudd, og basere sikkerhetsarbeid på resultater fra slike vurderinger målt opp mot nivå for akseptabel risiko.

Det er viktig at risikovurderingen blir en strukturert prosess, slik at man fanger opp de riktige risikofaktorene. Relevant underlagsdokumentasjon må være på plass og gjennomgås på forhånd og sentrale nøkkelpersoner må bidra i arbeidsmøter og lignende. Nøkkelpersoner kan være brukere av systemer og opplysninger (blant annet helsepersonell), jurister, informasjonssikkerhetspersonell, IKT-personell fra relevante fagområder (f.eks. server, nettverk), personvernrådgivere, og databehandlere/leverandører.

Ikke minst er slik deltagelse viktig for å kunne ivareta vurderinger knyttet til informasjonssikkerhet, personvern og pasientsikkerhet på tvers, for å kunne nå det overordnede målet om å yte forsvarlig helsehjelp.

Om vurderingene på tvers av fagområder etterlates til ledelsen i siste steg av vurderingene som gjøres, risikerer man å gå glipp av viktige perspektiver som må identifiseres tidlig i prosessen.

Eksempel:
Hjemmetjenesten i Normsund kommune skal anskaffe nytt system for elektronisk pasientjournal (EPJ), og må i den forbindelse gjennomføre en risikovurdering. Tjenesten har hatt utfordringer med sitt gamle EPJ-system, som hadde mye nedetid og dårlig tilgjengelighet for helsepersonell som var ute hos pasienter og brukere.

Det er derfor viktig å samle både helsepersonell som skal benytte systemet og IT-personell som kjenner de tekniske løsningene godt, for å få frem både systemets kritikalitet for helsehjelpen og potensielle tekniske risikoer som kan påvirke dette. Kommunens personvernrådgiver fra juridisk avdeling er med, sammen med informasjonssikkerhetsleder fra sikkerhetsavdelingen, for å få frem både krav og risikoer knyttet til disse fagområdene. Det er systemeier for hjemmetjenestens systemer som leder arbeidet med risikovurderingen, med bistand fra koordinator for virksomhetsstyring i kommunen, som eier kommunens risikometodikk.

Som underlag benyttes blant annet teknisk risikovurdering fra leverandør, teknisk skisse av planlagt installasjon/infrastruktur, beskrivelser av arbeidsprosesser for hjemmetjenesten, dokumentasjonskrav for helsepersonellet, lovkrav for informasjonssikkerhet og personvern fra Normen og trusselvurderinger fra nasjonale myndigheter. Merk at dette er et eksempel, og at andre forhold kan påvirke hvordan virksomheten organiserer sine risikovurderinger og anskaffelser.

2.3.1 Verdier

For å kunne definere hva som er informasjonsverdiene og hva som skal beskyttes mot uønskede hendelser må man vurdere verdien av ulike typer informasjon som virksomheten behandler.

I helse- og omsorgssektoren er dette er typisk ulike typer helse- og personopplysninger som behøves i en spesifikk prosess i virksomheten, som helseopplysninger i pasientjournal som er nødvendig for å yte helsehjelp og opplysninger om de ansatte som skal tilby riktig kompetanse til riktig tid. I tillegg til helse- og personopplysninger er det viktig å vurdere annen informasjon med betydning for informasjonssikkerheten, som er informasjon som ved uautorisert tilgang eller andre sikkerhetsbrudd vil medføre en risiko for virksomheten. Dette kan være blant annet konfigurasjonsfiler, resultat av risikovurderinger, beredskapsplaner, passordfiler og nettverkskart.

Behandlingsprotokollen og oversikten over systemer og teknologi vil være viktig underlagsdokumentasjon, for å kunne starte vurderingen av hvilken verdi de ulike informasjonstypene har for virksomheten.

Det vil være hensiktsmessig for mange å allerede i verdivurderingen se på hvilken verdi ulike informasjonstyper har for virksomhetens viktige prosesser, og vurdere hvorvidt det er konfidensielt, integritet og/eller tilgjengelighet som er mest sentralt. I mange tilfeller vil alle tre hovedaspektene av informasjonssikkerheten være viktige, men det vil ofte ikke være mulig å prioritere alle like høyt. Man bør også inkludere vurderinger av hvordan disse aspektene påvirker pasientsikkerheten.

Eksempel:
Hjemmetjenesten i Normsund kommune går gjennom sine informasjonsverdier i forbindelse med risikovurdering av nytt EPJ-system.

Helse- og personopplysningene om pasienter og brukere vurderes å være den aller mest kritiske verdien. Uten denne informasjonen i EPJ vil det være svært vanskelig å yte den nødvendige helsehjelpen på en forsvarlig helsehjelp.

De vurderer kritikaliteten ved å bruke ulike perspektiver, og kommer frem til følgende:

- Konfidensialitet: Det er sentralt å opprettholde helse- og personopplysningenes konfidensialitet for å ivareta både helsepersonells taushetsplikt og pasienter/brukeres personvern. Helseopplysninger er en særlig kategori av personopplysninger, som krever ekstra beskyttelse.
- Integritet: For å ivareta pasientsikkerheten, er det kritisk at helsepersonellet kan stole på at opplysningene i EPJ er korrekte og oppdaterte, ettersom pasienter vil behandles på bakgrunn av disse opplysningene.
- Tilgjengelighet: På samme måte er det kritisk at helsepersonellet har tilgang til opplysningene når de er ute hos pasient/bruker. Om disse ikke er tilgjengelige kan det påvirke pasientsikkerheten negativt.

De benytter en konsekvensskala som i kapittel 2.2.3 Akseptabel risiko som en støtte for å plassere de ulike informasjonsverdiene på riktig konsekvensnivå. Merk at disse vurderingene kun er eksempel på hvordan man kan gjennomføre en verdivurdering, og at virksomheten må gjøre sine egne vurderinger.

2.3.2 Trusler og risikoscenarioer

Når man har definert informasjonsverdiene, vurderer man hvilke trusler verdiene kan utsettes for. Trusler kan være både villede handlinger (snoking, kriminalitet, etterretning, mv.) og andre uønskede hendelser (menneskelig feil, uhell, teknisk svikt, ekstremvær, mv.). Åpne årlige trusselvurderinger fra Politiets sikkerhetstjeneste og Etterretningstjenesten, Nasjonal sikkerhetsmyndighets digitale risikobilder og rapporter fra HelseCERT kan være nyttig underlagsdokumentasjon, i tillegg til Direktoratet for e-helses overordnede risiko- og sårbarhetsvurdering.[15]

For å komme frem til hensiktsmessige scenarioer er det nyttig å idemyldre, gjerne ved å diskutere hvilke uønskede hendelser som kan true verdiene våre. Kjenner vi til hendelser som har inntruffet i virksomheten vår tidligere? Eller i lignende virksomheter? Dette kan være et godt sted å begynne.

Er pasientjournalene våre attraktive for kriminelle aktører som benytter løsepengevirus? Er fysiske servere plassert i områder der det ofte er flom? Man kan her søke å benytte scenarioer som kan true informasjonssikkerhet, personvern og pasientsikkerheten, for å få en tilstrekkelig forståelse av hvilken risiko helse- og personopplysningene er utsatt for. Ofte har man gjennomført lignende risikovurderinger tidligere, og kan hente inspirasjon fra disse.

Det kan være hensiktsmessig å fra begynnelsen av være bevisst på at de scenarioene man velger ut skal kunne dekke en bredde av risikoer. Et høyere antall scenarioer vil ikke nødvendigvis bidra til en bredere dekning av risikoen og gode risikoreduserende tiltak – det kan være nyttig å vurdere færre og mindre spesifikke scenarioer dersom disse er utformet for å inkludere særlig relevante risikoer. Scenarioene bør søke å dekke hendelser som truer både konfidensialitet, integritet og tilgjengelighet, og representere både villede handlinger og andre uønskede hendelser.

[15] Direktoratet for e-helse, Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren, 2019: https://www.ehelse.no/publikasjoner/overordnet-risiko-og-sarbarhetsvurdering-for-ikt-i-helse-og-omsorgssektoren

Se vedlegg 3.5 for en liste med eksempelscenarioer som kan være til inspirasjon for dette arbeidet. Den er ikke uttømmende, og alle oppfordres til å idemyldre og tilpasse til egen virksomhet.

Eksempel:
Hjemmetjenesten i Normsund kommune gjennomfører en trusselvurdering og definerer risikoscenarioer i forbindelse med risikovurdering av nytt EPJ-system.

De tar utgangspunkt i andre risikovurderinger som er gjennomført i helse- og omsorgstjenesten i kommunen, og beslutter å benytte en del av de samme scenarioene som er beskrevet der. Dette inkluderer blant annet snoking av helsepersonell uten tjenstlig behov, feilføring av helse- og personopplysninger i journal, og teknisk feil i tilgangsstyringen.

Kommunens sikkerhetsavdeling har fulgt med i nyhetsbildet og deltatt i kommunale informasjonssikkerhets-nettverk, og er derfor godt orientert om at løsepengevirus har rammet andre kommuner, inkludert helse- og omsorgstjenesten. De bestemmer seg for å inkludere et nytt scenario kalt «Løsepengevirus gjør EPJ-systemet utilgjengelig», der en opportunistisk trusselaktør har kryptert alle filene slik at de ikke er tilgjengelig for hjemmetjenesten. Merk at dette er et eksempel, og at det kan være andre scenarioer som er mer relevante for virksomheten.

2.3.3 Sårbarheter og eksisterende tiltak

Nasjonal sikkerhetsmyndighet beskriver sårbarheter som «forhold som en trusselaktør kan utnytte til å påvirke virksomhetens verdier». Eksempler på sårbarheter kan være feil eller mangler i design, prosedyrer, vedlikehold, opplæring og kommunikasjon.

Å vurdere sårbarheter som en del av en risikovurdering er å beskrive i hvilken grad eksisterende sikkerhetstiltak vil kunne hindre en trusselaktør i å kunne påvirke virksomhetens informasjonsverdier.[16] Det vil si hvilke menneskelige, teknologiske og organisatoriske tiltak virksomheten allerede har etablert som gjør det mindre sannsynlig at uønskede hendelser skjer eller at konsekvensene fra uønskede hendelser blir mindre alvorlig. Det kan være alt fra godt dokumenterte og innarbeidede rutiner for helsepersonell som skal benytte systemet til etablering av brannmurer og monitorering av nettverket.

I sin enkleste form kan dette være en diskusjon rundt bordet blant nøkkelpersonene som deltar i risikovurderingen, på grunnlag av tekniske skisser og risikovurderinger fra leverandør og det man vet om egne arbeidsprosesser i virksomheten. Funn fra diskusjonen bør dokumenteres som en del av risikovurderingen, og vil være nyttig i vurderingen av sannsynlighet og konsekvens.

2.3.4 Sannsynlighet

Når man har kommet frem til en liste med relevante scenarioer bør man vurdere sannsynligheten for at den uønskede hendelsen inntreffer, enten det er sannsynligheten for

[16] Nasjonal sikkerhetsmyndighet, Grunnprinsipper for sikkerhetsstyring: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/identifisere-og-kartlegge/avdekk-sarbarheter/

at en trusselaktør gjennomfører et suksessfullt angrep eller at flom oversvømmer serverrommet.

Man bør bruke en forhåndsdefinert skala for å vurdere sannsynlighet, som for eksempel definerer sannsynligheten etter frekvens (jo oftere en hendelse vil inntreffe, desto mer sannsynlig) eller etter tiltaksstyrke (jo mer effektive sikringstiltak, desto mindre sannsynlig).

Når man skal vurdere sannsynligheten for en fremtidig uønsket hendelse, vil det alltid være en viss grad av usikkerhet tilknyttet vurderingen. Om systemet et legekontor benytter for pasientadministrasjon gjennomsnittlig er nede 13 minutter per måned, vil man kunne beregne sannsynligheten med relativt høy treffsikkerhet. Det er imidlertid mange tilfeller der man ikke har tilstrekkelig gode data for å understøtte en vurdering av med hvilken frekvens en uønsket hendelse vil inntreffe.

Dette gjelder kanskje særlig når vi skal vurdere villede handlinger. Hvor sannsynlig er det for eksempel at opportunistiske organiserte kriminelle tar kontroll på akkurat ditt pasientjournalsystem for å true til seg løsepenger? Dette er det knyttet stor usikkerhet til, og det kan derfor gi større verdi i en sannsynlighetsvurdering å fokusere på hvorvidt det er enkelt å gjennomføre handlingen. Vil våre sikkerhetstiltak gjøre det mindre trolig at en trusselaktør lykkes?

Ofte vil det derfor være hensiktsmessig å benytte en skala for sannsynlighetsnivåer som beskriver sannsynlighet både med hensyn til frekvens og tiltaksstyrke. Det er hensiktsmessig at man benytter den samme skalaen på tvers av virksomheten slik at man kan aggregere risiko fra forskjellige områder, og at det er samme skala som er benyttet i arbeidet med akseptabel risiko som benyttes i risikovurderingen. Se vedlegg 3.2 for et eksempel på hvordan en slik skala kan se ut.

2.3.5 Konsekvens

Konsekvensen vurderes ved å se på hvor alvorlig det vil være for virksomheten dersom den uønskede hendelsen beskrevet i scenarioet skjer. Dette henger tett sammen med verdivurderingen – ofte kan man si at jo høyere verdi, desto mer alvorlig konsekvens.

Man bør bruke en forhåndsdefinert skala for å vurdere konsekvens, og disse har ofte eksempler både for konfidensialitet, integritet og tilgjengelighet. Se vedlegg 3.3 for et eksempel på hvordan en slik skala kan se ut.

Konsekvenser kan gjerne kategoriseres i ulike grupper, som f.eks. liv og helse, pasientsikkerhet, økonomi, lover og regler, tjenesteleveranse, mv. Konsekvens for de registrerte i personvernsammenheng kan også være en slik kategori. Kategoriene må tilpasses typen virksomhet og hvilke prosesser som er sentrale for tjenesteleveransene, og ikke minst hvilke andre kategorier som benyttes i risikovurderinger på andre områder enn informasjonssikkerhet.

Det kan være hensiktsmessig å vurdere både verstefallskonsekvenser og mer vanlige typer konsekvenser i ulike scenarioer og ved ulike hendelser.

2.3.6 Risiko

Risiko er ofte definert som sannsynlighet for at den uønskede hendelsen skal inntreffe ganget med konsekvensene hendelsen vil medføre. Man vil typisk illustrere risikoen ved å sette inn de ulike scenarioene i en risikomatrise, med grønne, gule og røde felter. Disse

signaliserer hvorvidt en risiko er av lav, middels eller høy karakter. Man må så vurdere om det er noen av disse risikoene som er på et for høyt nivå til at man kan akseptere det. Dersom det er tilfelle (typisk vil det nærmest alltid være det om man havner på rødt nivå), må man vurdere hvilke risikoreduserende tiltak man kan iverksette.

Det er hensiktsmessig at man benytter den samme risikomatrisen på tvers av virksomheten slik at man kan aggregere risiko fra forskjellige områder, blant annet fra arbeid med pasientsikkerhet, HMS, personellsikkerhet eller andre områder, og at det er samme matrise som er benyttet i arbeidet med akseptabel risiko som benyttes i risikovurderingen.

Det er knyttet usikkerhet til alle risikovurderinger da man gjør vurderinger av mulige hendelser frem i tid. Det er derfor viktig å synliggjøre kunnskapsgrunnlaget som ligger til grunn for ulike deler av vurderingen. Når du beskriver risikoen bør du også beskrive hvor sikker du er på vurderingen, for å sikre at de som skal beslutte eventuelle tiltak vet hvilket grunnlag risikoen er vurdert på. Det kan enten gjøres som en del av oppsummeringen av eller innledningen i risikovurderingen, eller som en beskrivelse knyttet til hvert scenario dersom det er mer hensiktsmessig (for eksempel dersom usikkerheten varierer veldig mellom ulike scenarioer).

Tabellen som følger viser et eksempel på en risikomatrise med sannsynlig og konsekvens, avmerket med grønne, gule og røde felter. Merk at dette er et eksempel, og enhver virksomhet må selv vurdere hva som er hensiktsmessige nivåer for egen risiko.

Eksempel:
Hjemmetjenesten i Normsund kommune gjennomfører risikovurdering av nytt EPJ-system.

De har blant annet valgt seg ut scenarioet «Løsepengevirus gjør EPJ-systemet utilgjengelig», og skal vurdere hvor sannsynlig det er at hendelsen inntreffer og hvor alvorlige konsekvenser den få for at de skal kunne levere forsvarlig helsehjelp.

Vurdering av sannsynligheten: Hjemmetjenesten i kommunen er kjent med at hendelsen har inntruffet i andre kommuner, det er derfor ikke utenkelig at det vil inntreffe hos dem. Det er ikke trolig at angrep har vært målrettede mot spesifikke kommuner, og det er derfor like sannsynlig at det kan skje i Normsund som i andre kommuner. Kommunen er imidlertid nå bedre kjent med angrepsmetoden, og har allerede etablert noen tiltak for å øke sin egen motstandskraft. Sannsynligheten vurderes på nivå 3 Mulig.

Vurdering av konsekvensen: Hjemmetjenesten er kjent med at hendelsen fikk alvorlige konsekvenser for helse- og omsorgstjenestene som har blitt angrepet, som måtte klare seg med helt manuelle rutiner uten EPJ-systemet. På grunn av tidligere tilgjengelighetsproblematikk med systemet har de etablert gode nødrutiner og er til en viss grad trent på å håndtere tjenesten manuelt. Konsekvensen vurderes på nivå 4 Alvorlig.

Risikoen i scenarioet for hjemmetjenesten i Normsund ender vurderes i rød sone, markert med en X i risikomatrisen under. Merk at denne vurderingen er et eksempel på bruk av metodikken, og at virksomheten må gjøre egne vurderinger basert på eget faktagrunnlag.

	5 Svært sannsynlig					
Sannsynlighet	4 Sannsynlig					
	3 Mulig				X	
	2 Mindre sannsynlig					
	1 Usannsynlig					
Risikomatrise		1 Ubetydelig	2 Lav	3 Moderat	4 Alvorlig	5 Svært alvorlig
		Konsekvens				

2.3.7 Risikoreduserende tiltak og risikoaksept

Ideelt sett skal alle virksomhetsmål nås uten at uønskede konsekvenser oppstår. Det vil imidlertid alltid være sannsynlighet for at uønskede hendelser inntreffer, og risikoeier må ofte velge mellom å etablere sikringstiltak, akseptere risiko og å la være å gjøre aktiviteter som innebærer for høy risiko.

Det er ledelsens ansvar å beslutte hvorvidt man kan akseptere risiko. Fagpersoner kan gjennomføre risikovurderingene, men det er virksomhetens leder og/eller en annen forhåndsdefinert risikoeier som beslutter risikoaksept som en del av risikostyringen.

Det er viktig at risikovurderingen har god kvalitet som beslutningsgrunnlag, og ikke minst at lederen er i stand til å se vurderinger av informasjonssikkerhet, pasientsikkerhet og personvern i sammenheng, for å ta beslutninger som sørger for forsvarlig helsehjelp og forsvarlige helse- og omsorgstjenester. Den som skal ta beslutningen må kjenne til virksomhetens akseptkriterier og relevante sikkerhetsmål, for å kunne ta disse beslutningene på forsvarlig vis.

Eksempel:
Normveien Psykologpraksis har gjennomført en oppdatering av risikovurderingen av sitt pasient-administrative system (PAS), og ser at et av scenarioene fra risikovurderingen nå befinner seg i den røde delen av risikomatrisen – det har høy risiko. I henhold til Normveiens akseptkriterier, må høy risiko håndteres på følgende måte:

Risikonivå	Kriterier for å akseptere risiko
Høy	Det er gjennomført et systematisk og svært grundig arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak.
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av daglig leder i Normveien Psykologpraksis. Aksept skal begrunnes og dokumenteres.

Psykologen som har ledet arbeidsgruppen for risikovurderingen rådfører seg derfor først med de andre tre medlemmene, og blir enig med de andre om å søke råd fra kontaktpersonen de har hos leverandøren av PAS. Hun bidrar med to tekniske tiltak som kan bidra til å redusere risikoen. Videre kommer helsesekretæren med et innspill til hvordan han kan endre en av arbeidsprosessene rundt timebooking, som også kan ha risikoreduserende effekt.

Psykologen dokumenterer det foreslåtte, og går til daglig leder for å legge frem arbeidsgruppens funn. Hun vurderer at den høye risikoen i utgangspunktet ikke kan aksepteres, og at de foreslåtte tiltakene skal gjennomføres.

Endringen i arbeidsprosessen kan implementeres umiddelbart, men de to tekniske tiltakene vil medføre en noe større ekstra kostnad. De kan derfor ikke gjennomføres innenfor nåværende budsjett, og må vente til årsskifte om tre måneder.

På grunn av at de ikke vil kunne gjennomføre pasientadministrasjon på en hensiktsmessig måte – og dermed yte forsvarlig helsehjelp – uten dette systemet, og siden det bare er tre måneder til tiltakene kan gjennomføres, vurderer daglig leder at nytten ved tjenesten er større enn risikoen. Normveien Psykologpraksis kan akseptere den røde risikoen på en midlertidig basis. Beslutningen, og vurderingen som ligger til grunn, dokumenteres og lagres sammen med risikovurderingen.

Merk tilsynsmyndigheter som f.eks. Datatilsynet og Helsetilsynet vil ha en kontrollerende tilsynsmyndighet, de vil da kunne gi pålegg om sikring av personopplysninger og herunder fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.

Merk at vurderingene i dette eksempelet kun er for å illustrere metodikken. Virksomheten må selv vurdere og håndtere risiko i henhold til egne akseptkriterier.

Dersom risikoen i et gitt scenario ikke kan aksepteres, må risikoeier vurdere risikoreduserende tiltak. Tiltak kan redusere risikoen både ved å redusere sannsynligheten for at en hendelse inntreffer, eller ved å redusere konsekvensen dersom hendelsen først har skjedd. Risikoreduserende tiltak kan være av menneskelig, teknologisk eller organisatorisk art.

Et eksempel på et menneskelig tiltak kan være kompetanseheving for helsepersonell som skal bruke en løsning, et teknologisk kan være å øke frekvensen på back-up på systemer som er kritiske for å yte helsehjelp, mens et organisatorisk tiltak kan være å etablere nye roller med ansvar for hele eller deler av en gitt prosess som tilgangsstyringsprosessen.

En risikobasert tilnærming krever at tiltak skal gjennomføres på grunnlag av risikovurderinger, og at man må vurdere kost/nytte før man beslutter hvilke tiltak som skal implementeres. Dersom planlagte tekniske tiltak for å oppnå akseptabel risiko ikke kan innføres umiddelbart, bør risikoreduserende administrative tiltak f.eks. i form av rutine vurderes. Det bør utarbeides en tiltaksplan, med ansvarlige og frister, for å sikre at besluttede tiltak iverksettes.

Eksempel:
Hjemmetjenesten i Normsund kommune gjennomfører risikovurdering av nytt EPJ-system. Scenarioet «Løsepengevirus gjør EPJ-systemet utilgjengelig» er vurdert å være en rød risiko.

Helse- og personopplysningene i hjemmetjenestens EPJ er sentral for å ivareta både informasjonssikkerhet, personvern og pasientsikkerhet. Kommunen benytter nivåer for akseptabel risiko i sin risikostyring, og for dette systemet skal risikoen være på grønt nivå. Derfor kan ikke hjemmetjenesten akseptere en risiko som er høyere enn grønn i matrisen kommunen deres bruker.

Sannsynlighet	5 Svært sannsynlig					
	4 Sannsynlig					
	3 Mulig				Risiko i scenarioet	
	2 Mindre sannsynlig		Akseptabel risiko			
	1 Usannsynlig					
Risikomatrise		1 Ubetydelig	2 Lav	3 Moderat	4 Alvorlig	5 Svært alvorlig
		Konsekvens				

Siden risikoen er rød, må beslutningen om eventuell risikoaksept eskaleres til kommunens øverste ledelse. Ledelsen får risikovurderingen presentert, og beslutter at det må gjennomføres tiltak for å redusere risikoen i dette scenarioet – den er for høy til at virksomheten kan akseptere den.

Det vil ikke være mulig å redusere denne risikoen til null, så tiltak av menneskelig, teknologisk og organisatorisk art må sikte på å redusere restrisikoen til et akseptabelt nivå. Merk at denne vurderingen er et eksempel for å illustrere metodikken, og ikke en fasit på hvilken risiko virksomheten kan akseptere i dette scenarioet.

Det vil som regel alltid være en viss restrisiko igjen etter en gjennomført risikovurdering og tiltaksplan. Målet er ikke å få risikoen ned i null, men å få risikoen ned på et nivå der man kan akseptere å leve med den.

2.4 Vurdering av personvernkonsekvenser

Virksomheter skal alltid vurdere hvilke konsekvenser behandling av helse- og personopplysninger medfører for den registrerte, som er det individet som opplysninger kan knyttes til. Virksomheten skal dokumentere lovligheten av behandlingen, formålet, hvordan personvernet til den registrerte er ivaretatt, og at det er gjort tilstrekkelige tiltak for å håndtere risikoen. Dette er krav som personvernforordningen stiller for alle behandlinger av personopplysninger.

Behandlingsprotokollen vil være et godt utgangspunkt for å vurdere flere av disse aspektene. Noen virksomheter velger også å legge til mer informasjon enn det lovkravet legger opp til i behandlingsprotokollen, for å skape større nytteverdi for vurderinger av personvernkonsekvenser og andre risikovurderinger.

Hvis det er sannsynlig at en behandling medfører høy risiko for de registrerte, skal virksomheten gjennomføre en mer grundig personvernkonsekvensvurdering, også kalt DPIA (Data Protection Impact Assessment). Denne vurderingen handler blant annet om å dokumentere at eventuell risiko for den registrerte ikke overgår den nytten som behandlingen av opplysningen kan gi, altså å dokumentere en forholdsmessighet. Videre er det sentralt at man ikke behandler flere personopplysninger enn det som er nødvendig.

Enhver virksomhet i helse- og omsorgssektoren skal vurdere om noen av behandlingene som planlegges (eller gjennomføres) vil føre til høy risiko for de registrerte. Den som har besluttet behandlingen må også ta ansvar for at nødvendig vurdering gjennomføres. Selv om bistand kan innhentes, må selve vurderingen gjennomføres av personer som har innsikt i fagområdet og hvordan virksomheten opererer.

Eksempel:
Normland kommune skal implementere elektronisk medisineringsstøtte. Medisindispenseren plasseres hjemme hos brukerne hvor et fjernpleiesystem gjør det mulig for ansatte å sjekke om pasienten/brukeren har tatt medisinene som de skal. Normland ønsker å forbedre pasientsikkerheten ved at pasienten/brukeren får rett medisin til rett tid og håper at medisinavvikene går ned.

Normland kommune gjør flere vurderinger (bl.a. risikovurdering, helsefaglige vurderinger) for å sikre at løsningen ivaretar krav til informasjonssikkerhet og personvern. De vurderer konsekvensene for personvernet til pasienten/ brukeren, om de har behandlingsgrunnlag og et klart formål og om det er nødvendig å gjennomføre en DPIA etter personvernforordningens artikkel 35. Kommunen gjennomfører den overordnende vurderingen. De vurderer at:

- innføringen av medisindispenserne ikke er en ny prosess da hjemmetjenesten i mange år har jobbet med medisineringsstøtte. Teknologien settes opp med en integrasjon til EPJ. Prosessen inkluderer ikke bruk av forsystem i en skytjeneste
- løsningen ikke samler inn nye personopplysninger om pasientene enn det de allerede gjør.
- personopplysningene som behandles ikke er så omfattende.
- teknologien ikke er ny siden dette er blitt brukt i mange andre kommuner
- leverandør får tilgang til opplysningene som registreres i teknologien
- det behandles helseopplysninger i form av type medisiner som kan avsløre et helseforhold.
- det ikke blir inngripende kontakt mellom tjenesten og pasient/bruker. Dersom pasienten/ brukeren ikke tar medisin som planlagt vil dette følges opp av hjemmetjenesten som normalt.

På bakgrunn av vurderingen inngår de en dekkende databehandleravtale og konkluderer med at det ikke er behov for å gjennomføre en DPIA etter artikkel 35. De dokumenterer konklusjonene sine. Merk at dette er et eksempel på hvordan denne vurderingen kan gjennomføres.

Datatilsynet har utarbeidet en oversikt over behandlingsaktiviteter som alltid krever at det må gjøres en DPIA, og virksomheten bør gjøre seg kjent med denne i forkant av oppstart av nye behandlinger av helse- og personopplysninger.[17] Det er videre hensiktsmessig om virksomhetens leder gjør en vurdering av hvorvidt det er ønskelig med flere virksomhetsspesifikke kriterier, som for eksempel sier at ved behandling av

[17] EU, About Article 29 Working Party, https://ec.europa.eu/newsroom/article29/items/59485/en; Datatilsynet, Når må man gjennomføre en vurdering av personvernkonsekvenser?, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/

helseopplysninger til forskning skal det alltid gjennomføres en DPIA uansett størrelsesorden, metode eller andre kriterier som eventuelt måtte inntreffe.

Vurderingene som gjøres i en DPIA skal ta utgangspunkt i den registrertes perspektiv, i motsetning til tradisjonelle risikovurderinger som benytter virksomhetsperspektivet. Hvordan påvirker vår behandling av helse- og personopplysninger de som opplysningene handler om? Derfor bør man også innhente synspunkter på den planlagte behandlingen fra de registrerte eller representanter for disse. Om man ønsker å forske på en spesifikk pasientgruppe kan man for eksempel undersøke om gruppen har en interesseorganisasjon som kan bidra med innhenting av denne typen innspill.

Man kan gjøre en DPIA i forkant, samtidig og/eller i etterkant av en risikovurdering av informasjonssikkerheten. Disse vurderingene vil uansett måtte sees i sammenheng, og som et minimum bør den vurderingen som ferdigstilles først oppdateres etter at den andre er ferdig, for å sikre at alle relevante risikomomenter er ivaretatt.

Dokumentasjonen som gjøres i en DPIA vil være viktig for å synliggjøre etterlevelse av virksomhetens arbeid med personvern, og er en sentral del av risikostyringen av informasjonssikkerhet og personvern i helse- og omsorgssektoren, så vel som den totale internkontrollen.

Det finnes flere ulike varianter av maler for vurdering av personvernkonsekvenser i bruk i helse- og omsorgssektoren i dag, blant annet fra Direktoratet for e-helse og fra KiNS/Bærum kommune.

Som beskrevet i kapittel 2.3 Risikovurdering er det også viktig her at vurderingen av personvernkonsekvenser blir en strukturert prosess, slik at man fanger opp de riktige risikofaktorene. Man må ha relevant underlagsdokumentasjon på plass og sentrale nøkkelpersoner må bidra i arbeidsmøter og lignende. Nøkkelpersoner kan være brukere av systemer og opplysninger (blant annet helsepersonell), jurister, sikkerhetspersonell, IKT-personell, personvernrådgivere, og databehandlere/leverandører.

Ikke minst er dette viktig for å kunne ivareta vurderinger knyttet til informasjonssikkerhet, personvern og pasientsikkerhet på tvers, for å kunne nå det overordnede målet om å yte forsvarlig helsehjelp. Om dette etterlates til ledelsen i siste steg av vurderingene som gjøres, risikerer man å gå glipp av viktige perspektiver som bør identifiseres tidlig i prosessen.

Datansvarlig skal rådføre seg med virksomhetens personvernombud (dersom virksomheten har PVO) i forbindelse med utførelsen av en DPIA. En negativ tilbakemelding fra personvernombudet betyr at man eventuelt bør gjøre tilpasninger i den planlagte behandlingen av helse- og personopplysninger for å oppnå ønsket formål innenfor regelverket. Med andre ord bør man vurdere om det for eksempel vil være mulig å bruke færre helse- og personopplysninger enn først planlagt, eller å beskytte dem på en annen måte, og slik kunne implementere en ny løsning på en litt mer personvernvennlig måte som likevel fyller det opprinnelige behovet for å yte forsvarlig helsehjelp.

Anbefalinger fra personvernombudet er imidlertid ikke siste stopp i prosessen med en vurdering av personvernkonsekvenser. Det er viktig å fremheve at det ikke er personvernombudets rolle å godkjenne en DPIA. Personvernombudet er en rådgiver, mens det bare er virksomhetens ledelse og/eller en forhåndsdefinert risikoeier som kan beslutte hvorvidt virksomheten kan akseptere konkrete personvernkonsekvenser og et gitt risikonivå på personvernområdet.

Endringshistorikk

Dato	Versjon	Endring
02.12.21	1.0	Ny veileder bygger på oppdatert innhold fra faktaarkene: - Faktaark 04 – Kartlegge og klassifisere systemer; - Faktaark 05 – Fastsette nivå for akseptabel risiko; - Faktaark 07 – Risikovurdering; i tillegg til nyutviklet materiale om relevante temaer innen risikostyring, inkludert vurdering av personvernkonsekvenser.
26.09.22	1.1	Beskrivelser tilknyttet akseptabel risiko er oppdatert iht. oppdatert krav i Normen 6.1. Endringer i følgende kapitler: - 1.2 Tema for veilederen - 1.4 Krav i Normen - 2.2.2 Oversikt over systemer og teknologi - 2.2.3 Akseptabel risiko - 2.3.7 Risikoreduserende tiltak og risikoaksept - 3.4 Eksempel på akseptkriterier for risiko Hoveddelen av endringene er gjort i kapittel 2.2.3 og 2.3.7.

3 Vedlegg

3.1 Eksempler på prioritering av systemer

Tabellen som følger viser hvordan ulike typer virksomheter kan prioritere sine systemer. Merk at dette er eksempler, og at enhver virksomhet må gjøre konkrete vurderinger av hvilke terskler man skal ha for ulike prioriteringsnivå og hvor lang avbruddstid man kan akseptere. Det som er viktig er at man gjør en bevisst og risikobasert prioritering av ulike systemer.

Type virksomhet	Med utgangspunkt i virksomhetens behandlingsprotokoll kan systemer prioriteres som følger:
Store virksomheter (f.eks. sykehus, kommuner, mv.)	• **Prioritet 1:** Systemer hvor stopp av tjeneste er eller kan være livstruende for pasient, inkludert feilbehandling av pasient, eller kritisk for virksomhetens drift • **Prioritet 2:** Systemer hvor stopp av tjeneste kan få alvorlige konsekvenser, f.eks. medføre betydelig merarbeid for personell, tapt effektivitet i virksomheten • **Prioritet 3:** Systemer hvor stopp av tjeneste kan føre til svekkelse av pasientens tillit • **Prioritet 4:** Systemer hvor stopp inntil 72 timer kan aksepteres • **Prioritet 5:** Systemer som ikke er prioritert Ledelsen beslutter krav til tilgjengelighet for de ulike prioritetene, som et minimum hva som er akseptabel avbruddstid. Det skal også kartlegges hvilke andre systemer de prioriterte systemene er avhengig av. Disse skal ha samme prioritet som de prioriterte systemene.
Mindre virksomheter (f.eks. rehabilitering- og opptrenings-virksomheter)	• **Prioritet 1:** Systemer hvor stopp av tjeneste er eller kan være livstruende for bruker/pasient inklusive feilmedisinering, eller kritisk for virksomhetens drift • **Prioritet 2:** Systemer hvor stopp av tjeneste kan få alvorlige konsekvenser, f.eks. medføre - tapt tillit hos bruker - betydelig merarbeid for personell - tapt effektivitet • **Prioritet 3:** Systemer hvor stopp inntil 24 timer kan aksepteres Ledelsen beslutter krav til tilgjengelighet for de ulike prioritetene, som et minimum hva som er akseptabel avbruddstid.
Små virksomheter	• **Prioritet 1:** Systemer hvor helse- og personopplysninger skal være tilgjengelig når behandlende personell har tjenstlig behov for dem

(f.eks. legekontor, tannlegekontor, fysioterapeutpraksis, psykologfellesskap, kiropraktor, manuellterapeut, bedriftshelsetjeneste)	Ledelsen beslutter at man for systemer med prioritet 1 som et minimum ikke kan akseptere tap av data.

3.2 Eksempel på sannsynlighetsnivåer

Tabellen som følger viser et eksempel på en skala for ulike sannsynlighetsnivåer, fremstilt som både frekvens og tiltaksstyrke. Merk at dette er et eksempel, og enhver virksomhet må selv vurdere hva som er hensiktsmessige terskelverdier for egen situasjon. Denne skalaen benytter fem nivåer, men flere virksomheter benytter også fire nivåer i sine skalaen. Virksomheten må selv velge hva som er hensiktsmessig med tanke på egenart og behov – og ikke minst for å kunne sammenligne risiko på tvers i virksomheten.

Eksempel på skala for sannsynlighet		
Sannsynlighets-nivå	**Frekvens** **(hvor ofte skjer det?)**	**Til støtte for vurdering av sannsynlighetsnivå: Tiltaksstyrke** **(hvor lett kan en uønsket hendelse skjer?)**
1 Usannsynlig	En gang hvert 5. år eller sjeldnere	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten • Tiltakene kan kun omgås/brytes av egne medarbeidere med gode ressurser, og god/ fullstendig kjennskap til tiltakene • Eksternt personell kan ikke omgå/bryte tiltaket
2 Mindre sannsynlig	En gang hvert år	• Sikkerhetstiltak er etablert i forhold til sikkerhetsbehovet og fungerer etter hensikten • Tiltakene kan likevel omgås/brytes av egne medarbeidere med normale ressurser, som i tillegg har normal kjennskap til tiltakene • Eksternt personell trenger gode ressurser, og god/fullstendig kjennskap til tiltakene for å omgå/bryte disse
3 Mulig	En gang hver måned	• Sikkerhetstiltak er ikke fullt etablert, eller fungerer ikke etter fullt ut etter hensikten • Egne medarbeidere trenger kun normale ressurser for å omgå/bryte tiltakene – det er ikke nødvendig med kjennskap til tiltakene • Eksternt personell trenger normal kjennskap til tiltakene (eksempelvis til hvilke prosedyrer som gjelder, eller hvordan sikkerhetsteknologi er implementert) – i tillegg til små/normale ressurser
4 Sannsynlig	En gang hver uke	• Sikkerhetstiltak er ikke etablert, eller • Det er kjent at tiltakene omgås/brytes av egne medarbeidere • Kan omgås/brytes av eksternt personell med normale ressurser og uten kjennskap til tiltakene
5 Svært sannsynlig	Daglig eller oftere	• Sikkerhetstiltak er ikke etablert, eller • Det er kjent at tiltakene omgås/brytes eksternt personell med normale ressurser uten kjennskap til tiltakene

3.3 Eksempel på konsekvensnivåer

Tabellen som følger viser et eksempel på en skala for ulike konsekvensnivåer, og hva disse kan være innen tilgjengelighet, konfidensialitet og integritet. Merk at dette er et eksempel, og virksomheten må selv vurdere hva som er hensiktsmessige terskelverdier for egen situasjon. Denne skalaen benytter fem nivåer, men flere virksomheter benytter også fire nivåer i sine skalaen. Virksomheten må selv velge hva som er hensiktsmessig med tanke på egenart og behov – og ikke minst for å kunne sammenligne risiko på tvers i virksomheten. Typisk vil virksomheter også ha konsekvensskalaer som omfatter andre områder, som blant annet liv og helse, omdømme, økonomi og brudd på spesielle regelverk.

Eksempel på skala for konsekvens	
Konsekvensnivå	**Eksempler angitt for tilgjengelighet, konfidensialitet og integritet**
1 Ubetydelig/ ingen	• Stans i tjenesteleveranse forekommer ikke • Intet uautorisert innsyn i helse- og personopplysninger • Journal er komplett • Ingen påvirkning på pasienters helse • Ikke brudd på personvernet • Ikke økonomisk tap • Ikke tap av omdømme
2 Lav	• Stans i tjenesteleveranse opptil 30 minutter • Uautorisert innsyn i enkelte helse- og personopplysninger og lovbrudd • Noen mangler i journal slik at helse- og personopplysninger ikke er fullstendige og ajourført i forhold til behandlingen av opplysningene • Ingen påvirkning på pasienters helse • Brudd på personvernet for et lite antall pasienter • Gjenopprettelig økonomisk tap • Noe midlertidig tap av omdømme ovenfor pasienten eller virksomheten
3 Moderat	• Stans i tjenesteleveranse opptil 2 timer • Uautorisert innsyn i flere helse- og personopplysninger, mulighet for endring og brudd på lov • Informasjon mangler i journal og brudd på lov • Det gis tilgang til en bruker fra en ekstern virksomhet som ikke har tjenstlig behov for EPJ for en eller flere pasienter • Skade, velferdstap eller påvirkning på pasienters helse • Brudd på personvernet for et moderat antall pasienter • Alvorlig økonomisk tap • Midlertidig eller moderat tap av omdømme ovenfor pasienten eller omgivelsene
4 Alvorlig	• Stans i tjenesteleveranse opptil 5 timer

	• Uautorisert innsyn i store mengder helse- og personopplysninger, mulighet for endring og brudd på lov • Viktig informasjon mangler i journal og brudd på lov • Det gis tilgang til en bruker fra en ekstern virksomhet som ikke har tjenstlig behov for EPJ for en eller flere pasienter • Alvorlig skade, velferdstap eller påvirkning for pasienters helse • Brudd på personvernet for et stort antall pasienter • Alvorlig økonomisk tap • Alvorlig tap av omdømme overfor pasienten eller omgivelsene
5 Svært alvorlig	• Stans i tjenesteleveranse mer enn 5 timer • Fullt uautorisert innsyn i eller mulighet for endring av alle helse- og personopplysninger og brudd på lov • Kritisk informasjon mangler i journal og brudd på lov • Medikament, dosering eller behandlingstiltak blir feilregistrert • Helse- og personopplysninger knyttes til feil person og fører til svært alvorlig påvirkning på pasienters helse • Tilgang til behandlingsrettet helseregister (inkl. EPJ) og helse- og personopplysninger kommer på avveie • Tap av liv • Svært alvorlig økonomisk tap • Svært alvorlig tap av omdømme

3.4 Eksempel på akseptkriterier for risiko

Følgende tabell er et eksempel på hvordan man kan strukturere hvem som kan akseptere risiko etter hvilke kriterier.

Risikonivå	Kriterier for å akseptere risiko
Lav	Kan aksepteres uten å vurdere alternative arbeidsmåter eller flere risikoreduserende tiltak.
	Aksepteres i tråd med etablerte nivåer i virksomheten, av risikoeier eller den som er delegert myndighet i linjen. Skal likevel dokumenteres i tilfelle endrede rammevilkår.
Moderat	Det er gjennomført et systematisk og grundig arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak.
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan aksepteres av risikoeier. Aksept skal begrunnes og dokumenteres.
Høy	Det er gjennomført et systematisk og svært grundig arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak.
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av virksomhetens øverste leder/ledelse. Aksept skal begrunnes og dokumenteres.

3.5 Eksempel på scenarioer

Følgende liste er eksempelscenarioer som kan være til inspirasjon for arbeidet med risikovurderinger. Den er ikke uttømmende, og alle som skal gjennomføre en risikovurdering anbefales å idemyldre blant deltagerne og tilpasse scenarioene til egen virksomhet.

Se kapittel 2.3.6 Risiko for et eksempel på hvordan et scenario kan formuleres og beskrives når man skal vurdere sannsynlighet og konsekvens.

KIT	Eksempel på scenario
K	Snoking, f.eks. helsepersonell som ser i journaler uten tjenstlig behov
K	Uautorisert tilgang til systemer med helse- og personopplysninger (tilsiktet, som følge av angrep eller lignende)
K	Uautorisert tilgang til systemer med helse- og personopplysninger (utilsiktet, pga. feil eller lignende)
K	Fysisk innbrudd/tyveri av opplysninger (utstyr)
K	Tilsiktet misbruk av sensitiv informasjon (for å presse/utnytte privatpersoner)
K	Tilsiktet misbruk av sensitiv informasjon (for å presse myndighetspersoner for politiske formål)
I	Uautorisert (mulighet for) endring av helse- og personopplysninger (tilsiktet, som følge av angrep eller lignende)
I	Uautorisert (mulighet for) endring av helse- og personopplysninger (utilsiktet, pga. feil eller lignende)
I	Helse- og personopplysninger knyttes til feil person i journal (feilføring)
I	Helse- og personopplysninger er ikke oppdaterte/feil i systemene
T	Tilsiktet og ikke-planlagte nedetider/utilgjengelighet på systemer (som følge av tjenestenektangrep, sabotasje, etc)
T	Utilsiktet nedetid på systemene (som følge av system- eller infrastrukturfeil, etc.)
T	Ikke tilgang til nødvendige helse- og personopplysninger eller annen kritisk informasjon (utilsiktet, som følge av feil etc.)
T	Ikke tilgang til nødvendige helse- og personopplysninger eller annen kritisk informasjon (tilsiktet, som følge av løsepengevirus eller andre typer angrep)
T	Brudd i kommunikasjon/funksjonalitet for sikker og rettidig deling av nødvendige helseopplysninger mellom samhandlende helsepersonell
T	Strømbrudd (fører til nedetid eller ødeleggelse)
T	Vannlekkasje (fører til nedetid eller ødeleggelse)
T	Naturkatastrofer og ekstremvær (fører til nedetid eller ødeleggelse)
KIT	Innsider benytter egne tilganger til andre formål (utro tjener)
KIT	Innsider benytter egne tilganger til andre formål som følge av press fra eksterne aktører (kriminelle, fremmede makter)
KIT	Innsider benytter egne tilganger til andre formål som følge av social engineering fra eksterne aktører (blir lurt, gjennom phishing eller andre teknikker)
KIT	Personell hos databehandler benytter tekniske tilganger til andre formål enn det som er regulert av databehandleravtalen
KIT	Menneskelig feil (utilsiktet)
	…