Informasjonssikkerhet og personvern for leverandører til helse- og omsorgssektoren

Versjon 1.0

Juni 2023

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

Innholdsfortegnelse

1. Innledning

1.1 Bakgrunn og tema for veilederen

Helse- og omsorgstjenesten er avhengig av private leverandører innen IKT-området, og sektoren ønsker at sikkerhetsutfordringen løses i fellesskap, i tråd med EU/EØS-krav og beste standard internasjonalt.

Denne veilederen er utarbeidet for å lette arbeidet med anskaffelser og leverandøroppfølging og bidra med kompetanseheving for å sikre at krav til Informasjonssikkerhet og personvern blir ivaretatt i anskaffelsesprosessen, innføring av teknologi og i den videre oppfølging av leverandør.

Veilederen skal gi veiledning til, og bidra til etterlevelse av kravene i Normen knyttet til anskaffelser og bruk av leverandører.

1.2 Målgruppe

Målgruppen er leverandører til helse og omsorgstjenesten, og ansatte hos virksomheter i helse- og omsorgstjenesten som forvalter og anskaffer teknologi og programvare.

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

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 gjennom avtale med virksomheten eller Norsk Helsenett SF.

1.3 Om Normen

Normen er en bransjenorm for informasjonssikkerhet og personvern for helse- og omsorgssektoren. Det er et sett med krav til virksomheter i sektoren for hvordan de skal jobbe med dette. Under Normen er det også utviklet veiledningsdokumenter som utdyper og supplerer kravene i bransjenormen.

Normen stiller krav som detaljerer og supplerer gjeldende regelverk. Den er likevel ikke heldekkende. Helseregisterloven, personopplysningsloven og annet regelverk stiller visse krav til behandling av helse- og personopplysninger utover det som er tema for Normen.

Normen skal blant annet styrke og forenkle arbeidet med informasjonssikkerhet og personvern, bidra til at virksomheter som følger Normen har egnede tekniske og organisatoriske tiltak på plass, fremme samhandling gjennom tillit i helse- og omsorgssektoren og bidra til god pasientsikkerhet og godt personvern.

Normen blir forvaltet av Styringsgruppen for Norm for informasjonssikkerhet og personvern.

1.4 Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk

Helsetjenesten er underlagt omfattende regulering gjennom lover, forskrifter, normer og standarder. IKT og utstyr som brukes i helsetjenesten må enten oppfylle disse kravene direkte eller gjøre det mulig for virksomheten å oppfylle dem. Utover nasjonal helselovgivning og personvernlovgivning kan følgende være relevant (listen er ikke uttømmende):

- NSM Grunnprinsipper for IKT-sikkerhet
- MDR - Regelverket for medisinsk utstyr
- NIS2 – direktivet
- MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices
- Lov om nasjonal sikkerhet (Sikkerhetsloven)
- Relevante ISO-standarder for informasjonssikkerhets- og personvern
- CIS Critical Security Controls

Leverandøren har et selvstendig ansvar å følge relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk.

1.5 Utvikling av veilederen

Utviklingen av denne veilederen er gjort i samarbeid med en referansegruppe bestående av fagpersoner fra helsesektoren innen IKT, medisinsk teknologi og innkjøp (både kommune og spesialisthelsetjenesten). Leverandører var godt presentert med kompetanse innen personvern, innkjøp, IKT og medisinsk teknologi.

1.6 Leseveiledning

Med systemer menes i denne veilederen elektroniske pasientjournaler, medisinske fagsystemer, merkantile systemer som understøtter pasientbehandling og Operasjonell teknologi som kan påvirke virksomhetens evne til å yte helsehjelp. Operasjonell teknologi (heretter OT) – omfatter systemer som regulerer og overvåker infrastruktur, logistikk og klima i en bygningsmasse.

Normen og en del annet lovverk bruker begrepet virksomhet og leverandør. Når det gjelder behandling av helse- og personopplysninger brukes begrepene dataansvarlig og databehandler. Denne veilederen bruker også begrepet kunde. Begrepene brukes om hverandre, der dette er hensiktsmessig ut fra kontekst.

2. Personvern, informasjonssikkerhet og taushetsplikt

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.

Informasjonssikkerhet handler om å håndtere risiko relatert til informasjon og behandling av personopplysninger. Informasjonens integritet, tilgjengelighet og konfidensialitet skal sikres. God informasjonssikkerhet er viktig for å kunne utøve forsvarlige helsetjenester. For å kunne håndtere risiko på en god måte, må alle avhengigheter i virksomheten inngå i risikovurderingen. Dette kan blant annet være IKT-løsninger, Medisinsk utstyr, og operasjonell teknologi (OT).

Personvern kan defineres og beskrives på ulike måter. Uansett hvilken innfallsvinkel som velges, står det enkelte menneskets ukrenkelighet og krav på respekt fra andre mennesker, respekt for egen integritet og privatlivets fred sentralt. Personvern er derfor nær knyttet til enkeltindividers muligheter for privatliv, selvbestemmelse og selvutfoldelse.

Tema for Normen og denne veilederen er den delen av personvernet som handler om personopplysningsvern. Personvernforordningen (GDPR) regulerer personopplysningsvernet. Personopplysninger skal behandles etter prinsippene i personvernforordningen art. 5 og de registrertes rettigheter skal sikres.

En viktig del av dette er det personvernforordningen art. 32 kaller personopplysningssikkerhet. Det er det samme som informasjonssikkerhet for personopplysninger. For å ivareta personvernet er det f.eks. viktig å ha solide informasjonssikkerhetstiltak på plass for å beskytte personopplysningene mot uautorisert tilgang eller lekkasjer. På samme måte er god kontroll på informasjonssikkerhet avhengig av respekt for personvernet og riktig behandling av personopplysninger.

Helselovgivningen har mange regler knyttet til behandlingen av helseopplysninger. Virksomheter i helse- og omsorgssektoren må sørge for at behandlingen av helse- og personopplysninger skjer i samsvar med både Personopplysningsloven og helselovgivingen.

2.1 Er leverandør det samme som databehandler?

Personvernforordningen definerer to viktige roller;

- Dataansvarlig er den som bestemmer formålet med behandlingen av helse- og personopplysninger og hvilke midler som skal benyttes.
- En databehandler er en virksomhet som behandler helse- og personopplysninger på vegne av dataansvarlig

En leverandør vil ha en begge rollene; både behandlingsansvarlig for personopplysninger som samles inn om egne ansatte og forretningskontrakter og databehandler når en behandler personopplysninger på vegne av kunder.

Svaret på spørsmålet i tittelen er altså at dersom en leverandør behandler personopplysninger på vegne av kunden så er den også en databehandler.

2.2 Noen utvalgte personvernområder

2.2.1 Personvernprinsippene

Personvernforordningen bygger på noen grunnleggende prinsipper som virksomheten må sørge for å ivareta når den behandler personopplysninger, se pvf art.5.

Dataansvarlig må sikre at egen virksomhet opptrer i henhold til personvernprinsippene.

Prinsippene gir uttrykk for både grunnleggende hensyn som personvernforordningen skal ivareta, og konkrete krav til hvordan personopplysninger skal behandles. Prinsippene er selvstendige regler som stiller krav til all behandling av personopplysninger. I tillegg skal de brukes i tolkningen av andre bestemmelser i forordningen og personvernbestemmelser i andre lover, herunder lover som regulerer behandling av personopplysninger i helse- og omsorgssektoren.

Personvernprinsippene består av:

- Prinsippene om lovlighet, rettferdighet og åpenhet
- Prinsippet om formålsbegrensning
- Prinsippet om dataminimering
- Prinsippet om riktighet
- Prinsippet om lagringsbegrensninger
- Prinsippet om integritet og konfidensialitet
- Prinsippet om ansvar

Les mer om i Normens faktaark om personvernprinisppene.

2.2.2 Formål og behandlingsgrunnlag

Dataansvarlig skal alltid definere ett eller flere formål med behandlingen av helse- og personopplysninger. Formålene skal være spesifikke, uttrykkelig angitte og legitime, og de skal dokumenteres i virksomhetens protokoll over behandlingsaktiviteter.

Hvis helse- og personopplysningene skal brukes til andre formål enn de som virksomheten definerte før innsamlingen, så må denne behandlingen i utgangspunktet ha et eget behandlingsgrunnlag.

Helse- og personopplysninger kan bare behandles når det finnes et lovlig grunnlag for å behandle dem. I personvernforordningen kalles dette behandlingsgrunnlag. Hvert formål skal ha et eget behandlingsgrunnlag. Det er dataansvarlig som har ansvar for å etablere et lovlig grunnlag.

Det finnes seks ulike behandlingsgrunnlag som virksomheten kan velge mellom. Behandlingsgrunnlagene er

- samtykke
- nødvendig for å oppfylle en avtale

- nødvendig for å oppfylle en rettslig forpliktelse
- nødvendig for å verne om vitale interesser
- nødvendig for å utøve en oppgave i allmenhetens interesse eller utøve offentlig myndighet
- nødvendig for formål knyttet til en berettiget interesse.

Les mer om i Normens faktaark om Formål og behandlingsgrunnlag

2.2.3 De registrertes rettigheter

Både personvernlovgivingen og helselovgivningen gir rettigheter til pasienter og de registrerte. Ved behandling av helseopplysninger i forbindelse med helsehjelp gjelder personvernforordningen og personopplysningsloven så langt ikke noe annet følger av pasientjournalloven. I pasientjournalloven vises det til bestemmelser i helselovgivningen og personvernforordningen.

Les mer rettigheter i Normens Veileder for rettigheter ved behandling av helse og personopplysninger

Databehandleravtalen skal blant annet pålegge leverandøren å bistå virksomheten i at den registrerte kan ivareta sine rettigheter. Dette skal sikre at leverandøren bidrar i ivaretakelsen av den registrertes rettigheter. Bistanden kan skje gjennom teknisk funksjonalitet eller annen praktisk bistand.

Databehandleravtalen eller tilhørende instrukser bør, beskrive hvordan leverandøren skal bistå i håndhevingen av en registrerts rettigheter. Virksomheten bør sørge for en tydelig ansvarsfordeling fra starten av, slik at henvendelser fra registrerte følges opp fortløpende. Virksomheten kan for eksempel spesifisere at leverandøren skal stå for innsamlingen av alle personopplysningene når virksomheten skal gi innsyn.

2.2.4 Innebygget personvern

Det er krav til at systemer og løsningen er utformet etter innebygget personvern (Privacy by design). Det går ut på å integrere personvern og personvernbeskyttende tiltak i systemets arkitektur og funksjonalitet fra start av. Dette sikrer at personvern blir en innebygd egenskap i løsningen.

Et viktig prinsipp innenfor Privacy by Design er dataminimering. Dette prinsippet handler om å begrense innsamlingen, bruket og lagringen av personopplysninger til det som er strengt nødvendig for det angitte formålet. Ved å redusere mengden personopplysninger som behandles, reduseres også risikoen for uautorisert tilgang eller misbruk av data.

Dataminimering innebærer å vurdere nøye hvilke typer personopplysninger som er nødvendige for å oppnå det ønskede formålet, og kun samle inn og behandle disse spesifikke opplysningene. Dette kan oppnås ved å implementere tekniske og organisatoriske tiltak som begrenser datainnsamlingen.

2.3 Taushetsplikt om helse og personopplysninger

Alle pasienter og brukere av helse- og omsorgstjenester har rett til vern mot spredning av opplysninger om personlige og helsemessige forhold.

Det er flere lovbestemmelser som regulerer dette og som har betydning for leverandørs taushetsplikt. Noen av disse er

- helsepersonelloven § 21 (helsepersonells taushetsplikt)
- spesialisthelsetjenesteloven § 6-1 (alle som utfører tjeneste for helseinstitusjon som omfattes av loven har taushetsplikt etter forvaltningsloven § 13)
- pasientjournalloven § 15 (alle som behandler helseopplysninger etter denne lov har taushetsplikt
- forvaltningsloven § 13 (enhver som utfører tjeneste for et forvaltningsorgan å hindre at andre får kjennskap til det han gjennom tjenesten får vite om noens personlige forhold og om tekniske innretninger, fremgangsmåter og forretningsforhold av konkurransemessig betydning)

Helsepersonells taushetsplikt innebærer både en plikt til å tie og en aktiv plikt til å hindre at uvedkommende får tilgang til taushetsbelagt informasjon. Virksomheter i helse- og omsorgstjenesten har et ansvar for å tilrettelegge arbeidet på en slik måte at helsepersonell reelt kan overholde taushetsplikten. Virksomheten skal sørge for at alt personell som gis tilgang til helse- og personopplysninger og annen informasjon underlagt taushetsplikt, er kjent med sin taushetsplikt.

Virksomheten skal legge til rette for at personellet ivaretar taushetsplikten. Dette bør minst sikres gjennom

- tilgangsstyring, logging og etterfølgende kontroll
- sikring av informasjonssystemer
- rutiner, opplæring og informasjon
- utforming av fysiske lokaler

Normen sier at en leverandør kan håndtere helse- og personopplysninger enten ved behandling på vegne av den dataansvarlige, ved tjenesteutsetting eller ved at det ytes f.eks. vedlikeholdstjenester som innebærer at leverandørens ansatte kan eksponeres for taushetsbelagt informasjon.

Normen sier videre at leverandøren skal forsikre at de har rutiner som pålegger alle medarbeidere taushetsplikt om helse- og personopplysninger og annen taushetsbelagt informasjon. Leverandøren kan selv administrere og oppbevare taushetserklæringer for eget personell, men den dataansvarlige skal sikres innsyn ved behov.

En annen aktuell taushetsplikt, som vi ikke omtaler her, er kundens taushetsplikt i anskaffelser. For offentlige anskaffelser har DFØ god veiledning.

3. Ansvar for å følge kravene i Normen

Den dataansvarlige har ansvaret for at krav til informasjonssikkerhet og personvern følges gjennom hele leveransekjeden. I leveranser av f.eks. tjenester, maskinvare eller systemer

skal det avtales skriftlig med leverandører hvilke sikkerhetskrav som skal oppfylles for at den dataansvarlige skal kunne oppfylle sitt ansvar. Hvilke av Normens krav som gjennom avtale gjelder for leverandører, er avhengig av hva slags type leveranse det er snakk om, for eksempel:

- databehandling, i form av for eksempel skytjenester eller driftstjenester
- vedlikehold, for eksempel ved fysisk service eller fjernaksess
- leveranse av løsninger og systemer

Avtalene skal inkludere forpliktelser om at partene skal oppfylle relevante krav og tiltak som følger av den til enhver tid gjeldende Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, samt regulering av sanksjoner ved brudd på denne, relevant lovgivning og avtalen for øvrig.

Kunden skal gjennom relevante avtaler forsikre seg om at leverandøren har tilfredsstillende styringssystem mht. sikkerhetsrevisjon og avviksbehandling.

Databehandler skal bare behandle helse- og personopplysninger, samt annen taushetsbelagt informasjon etter instruks fra dataansvarlig. Hvordan databehandler kan behandle data på vegne av dataansvarlig, skal reguleres i avtale.

Den dataansvarlige kan bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personopplysningsloven. Tilstrekkelige garantier betyr at databehandleren oppfyller kravene i lov og forskrift samt de kravene fra Normen som er relevante for det aktuelle avtaleforholdet.

Leverandører som er medlemmer i Helsenettet er forpliktet til å følge kravene i Normen gjennom Tredjepartsavtalen og medlemsvilkårene, les mer om dette i kapittel om Norsk helsenett. I anskaffelsesprosesser er det vanlig at det stilles krav til at løsningen eller leverandøren skal følge Normen, les mer om dette i kapittel om anskaffelser.

4. Risiko

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.

Risikostyring er koordinerte aktiviteter som har til hensikt å rettlede og kontrollere en organisasjon med tanke på risiko. Det omfatter å få oversikt over informasjon og teknologi i virksomheten, identifisere trusler, sårbarheter og konsekvenser ved mulige uønskede hendelser både for virksomheten og for registrerte personer, analysere risikoen og etablere tiltak for å opprettholde et egnet sikkerhetsnivå.

Normen sier at virksomhetene, innenfor lovverkets rammer, skal søke en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet. Risikostyring er et viktig

verktøy for å søke en slik balansert tilnærming, inkludert risikovurderinger av informasjonssikkerhet og vurderinger av personvernkonsekvenser.

Det skal tas hensyn til den tekniske utviklingen, gjennomføringskostnader og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i, når det vurderes om en risiko kan aksepteres. Arbeidet med risikostyring skal ta hensyn til for eksempel type og mengde opplysninger, virksomhetens størrelse og behandlingens kompleksitet.

En sentral del av risikostyringen 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.

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.

Eksempel:

Beskyttelse av opplysninger kan gjøres i systemet, eller det kan gjøres med fysisk begrensning av tilgangen til systemet. Det må vurderes når og hvordan et system benyttes. For et system som benyttes i forbindelse med akutte situasjoner, i et område som har tilgangskontroll og hvor det kun er ansatte som har tilgang, må det vurderes om det trenger å være like strenge krav til beskyttelse som til et system som står i et område med tilgangskontroll der publikum/pasienter kan få tilgang til systemet. Vurderingen må også ta høyde for hvor tidskritisk det er å få tak i opplysningene.

4.1 Risikovurdering (ROS)

Risikovurdering er et verktøy for å identifisere uønskede hendelser og for å implementere hensiktsmessige tiltak. Risikovurderingen bør ta utgangspunkt i en kartlegging av informasjonsverdier. I en risikovurdering vurderer man sannsynligheten for og mulige konsekvenser av at en hendelse inntreffer. Dersom risikoen er uakseptabel, skal virksomheten gjennomføre tiltak for å redusere risikoen.

Normen sier at det skal som minimum gjennomføres risikovurderinger før:

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

Risikovurderingen bør oppdateres når risikobildet endres. Dette betyr at man regelmessig bør vurdere risikoene knyttet til virksomheten, og oppdatere risikovurderingen i tråd med eventuelle endringer.

Når risikobildet endres, kan det oppstå nye trusler, teknologiske endringer, endringer i virksomhetens driftsmiljø eller andre faktorer som påvirker sikkerheten. Ved å oppdatere

risikovurderingen kan man identifisere og vurdere de nye risikoene og tilpasse tiltakene for å håndtere dem.

Oppdatering av risikovurderingen bør skje regelmessig og i samsvar med virksomhetens behov og risikoprofil. Dette kan være basert på en fast tidsplan, eller det kan være trigget av endringer i trusselbildet.

Risikovurderingen bør være en kontinuerlig og iterativ prosess, der man hele tiden evaluerer, oppdaterer og forbedrer håndteringen av risiko. Dette bidrar til å sikre at organisasjonen er proaktiv og robust i sitt arbeid med å håndtere risiko.

Risikovurderinger bør gjenspeile avhengigheter mot andre systemer. Tydelige avgrensninger bør også være på plass for å definere hva som er inkludert i vurderingen og hva som er dekket i andre vurderinger.

Det bør være et godt samarbeid mellom kunde og leverandør ved gjennomføring av risikovurdering. Begge parter har en interesse i at løsninger som er anskaffet kan tas i bruk. Leverandør bør vurdere å dele nødvendig informasjon for risikovurderinger tidlig i anskaffelsesprosessen og ellers samarbeide med kunden etter beste evne.

Risikovurderinger skal dokumenteres. Der det er nødvendig å gjennomføre tiltak for å oppnå akseptabel risiko, skal tiltakene fremgå av en plan med tydelig frist og hvem som er ansvarlig for gjennomføring. Planen skal forankres hos virksomhetens ledelse.

4.2 Personvernkonsekvensvurdering (DPIA)

Alle som behandler personopplysninger, skal vurdere konsekvenser av behandlingen for den registrerte. Virksomheten skal dokumentere lovligheten av behandlingen (behandlingsgrunnlag), 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. Hvordan disse ivaretas bør være en sentral del av virksomhetens internkontroll.

Dataansvarlig skal alltid vurdere hvilken risiko en behandling av personopplysninger gir for de registrertes rettigheter og friheter.

Hvis det er sannsynlig at en behandling medfører høy risiko for de registrerte, så skal den gjøre en personvernkonsekvensvurdering. En personvernkonsekvensvurdering (Data Protection Impact Assessment eller DPIA) skal sikre at personvernet til dem som er registrert i løsningen ivaretas. Dette er en plikt etter Personvernforordningen (GDPR) artikkel 35.

Personvernkonsekvensvurdering er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og beslutte risikoreduserende tiltak.

Personvernkonsekvensvurderinger skal minst inneholde:

- en systematisk beskrivelse av behandlingsaktivitetene av helse- og personopplysninger beskrivelse av formålet med behandlingen

- en vurdering av om behandlingene av helse- og personopplysninger er nødvendige og står i rimelig forhold til formålet
- en vurdering av risikoen for personvernet til den registrerte
- planlagte risikoreduserende tiltak for ivaretakelse av personvernet

Det anbefales å starte arbeidet med å kartlegge sentrale personvernspørsmål og vurdere ivaretakelse av rettigheter og friheter så tidlig som mulig og allerede før det foreligger et løsningskonsept. En slik tidlig overordnet vurdering av personvernspørsmål vil kunne fungere som underlag for å gjennomføre en personvernkonsekvensvurdering etter artikkel 35.

Det er ofte aktuelt å gjennomføre personvernkonsekvensvurderinger i forbindelse med anskaffelsesprosesser. Ved anskaffelser bør virksomheten starte med personvernkonsekvensvurderingen så tidlig som mulig, og gjerne sammen med at virksomhetens behov blir spesifisert. På denne måten kan prosessen med personvernkonsekvensvurderingen blant annet hjelpe virksomheten med å utforme krav i konkurransegrunnlaget. Det vil imidlertid være behov for å revidere personvernkonsekvensvurderingen underveis i den videre prosessen med anskaffelsen når virksomheten vet mer om hvordan den endelige løsningen vil se ut.

Leverandør som er databehandler skal bistå den behandlingsansvarlige i gjennomføringen av en DPIA og fremlegge all nødvendig informasjon,se pvf artikkel 28 nr. 3 bokstav f

Dersom mulig kan leverandør bistå med relevant informasjon om behandling av personopplysninger i DPIA allerede i en anskaffelsesprosess. Dette kan gjøre arbeidet med gjennomføring av DPIA lettere. Begge parter har interesse av at dette gjøres enklest mulig.

Det er flere gode veiledningssider og maler for personvernkonsekvensvurderinger. Les mer på nettsidene til blant annet Direktoratet for e-helses mal og veiledning, Datatilsynet eller KINS.

5. Avtaler og krav til oversikt og kontroll

5.1 Styringssystem/ internkontroll

Normen sier at «Den som har det overordnede ansvaret for en virksomhet, skal sørge for at det etableres og gjennomføres systematisk styring av virksomhetens aktiviteter (internkontroll).»

Internkontrollen skal være formalisert, og det er et krav i Normen at dokumentasjon om internkontrollen til enhver tid skal være oppdatert og lett tilgjengelig for alle ansatte. Det må også etableres rutiner for å sikre at styrende dokumenter til enhver tid er oppdaterte i tråd med krav i gjeldende lovverk, beslutninger, organisatoriske løsninger, rutiner og andre relevante styringsdokumenter. Informasjonssikkerhet og personvern bør inngå som en integrert del av den totale internkontrollen i virksomheten.

Leverandøren har som alle andre virksomheter i helse- og omsorgssektoren plikt til å dokumentere sitt eget ansvar og sin egen organisering av arbeidet med informasjonssikkerhet og personvern.

Kunden vil kunne ønske å verifisere at du tar informasjonssikkerhet på alvor og at dine underleverandører også implementerer passende tiltak for å beskytte informasjonen som de behandler.

Alle løsninger/prosesser som behandler personopplysninger skal inngå i styringssystemet.

Det finnes flere standarder og sertifiseringer som kan være gode verktøy for leverandører for å implementere og dokumentere styring og kontroll. En mye brukt standard er ISO 27001 og 27002. Kravene i Normen en mappet mot ISO 27001 og 27002. Les mer om dette på Oversikt over Normens krav og mapping mellom ISO, CCM og Normen – ehelse

5.2 Protokoll

Etter innføringen av personvernforordningen (GDPR) har også databehandler et nytt og selvstendig ansvar for å overholde regelverket. Dette er en endring fra det tidligere personverndirektivet, der den behandlingsansvarlige/ dataansvarlig var alene juridisk ansvarlige for å overholde kravene. Det gir dermed leverandører et utvidet ansvar for å ha og dokumentere oversikt.

Personvernforordningens regler viser at det er viktig å se på ansvaret for dataene i hele verdikjeden, fra kunden til tjenesteleverandøren og til involverte underleverandører. Dette gjøres blant annet gjennom plikten til å føre en oversikt over all behandling av personopplysninger, en protokoll over behandlingsaktiviteter, se personvernforordningen art. 30.

Behandlingsprotokollen er viktig for å ha og vise at man har oversikt over hva virksomheten behandler, hvilket formål de behandles for og hvem som behandler og har fått utlevert dataene. Den er også et viktig verktøy for å sikre de registrertes rettigheter.

Kunden skal føre protokoll over behandlinger av helse- og personopplysninger. Leverandør skal føre en protokoll over alle kategorier av behandlingsaktiviteter som utføres på vegne av kunden. Behandlingsansvarlig og databehandler har også plikt til å føre oversikt over IKT-systemer, infrastruktur, digitale tjenester og annen informasjon med betydning for informasjonssikkerheten, klassifisere systemene og kartlagt konsekvenser ved bortfall. For å kunne oppfylle sine forpliktelser og bistå oppdragsgiver med oppdrag som innsyn, sletting og retting er en avhengig av en komplet oversikt over IKT-systemene.

Les mer om protokoll i Normens faktaark om protokoll.

5.3 Kontrakt

Det kan være variasjon i bruken av kontrakter i forbindelse med leveranser av utstyr og systemer til helse- og omsorgssektoren. Det er variasjon i kontraktens innhold og på hvilket tidspunkt kontrakter inngås. For at leverandører skal kunne etterleve krav eller unngå å godta krav som kan oppfattes som urimelige, er det viktig at utkast til kontrakt blir en del av anskaffelsesdokumentene. I anskaffelsesprosessen fastlegges rammene for avtalens innhold, og det er oppdragsgiver som legger premissene for innholdet. Det er også oppdragsgiver som stiller kravene som leverandørene skal svare på, inkludert krav til datasikkerhet og behandling av personopplysninger. Kontrakten fordeler risiko og angir partenes ansvar og forpliktelser i avtaleperioden.

Direktoratet for økonomistyring har mange standardavtaler (SSA) som er tilpasset forskjellige leveransemodeller og prosesser. Det anbefales at disse benyttes i forbindelse med

leveranser til helse- og omsorgssektoren. Det er viktig at kontrakten fordeler risiko og angir partenes ansvar og forpliktelser i avtaleperioden. Det er også viktig at kravene i kontrakten kan etterleves av begge parter.

https://anskaffelser.no/anskaffelsesprosessen/anskaffelsesprosessen-steg-steg/avklare-behov-og-forberede-konkurransen/spesifikasjoner-krav-kriterier-og-kontraktsvilkar/kontrakt-og-kontraktsvilkar

5.4 Databehandleravtaler

Dataansvarlig har ansvar for å inngå en databehandleravtale med leverandøren dersom leverandøren skal drifte IT-tjenester eller får tilgang til helse- og personopplysninger. Databehandleravtalen skal inneholde vilkår for hvordan databehandleren kan behandle helse- og personopplysninger og skal regulere hva databehandler kan og skal gjøre.

Avtalen sikrer at helse- og personopplysninger ikke brukes til andre formål enn det dataansvarlig/behandlingsansvarlig ønsker og at nødvendige tekniske og organisatoriske sikkerhetstiltak følges av databehandleren.

Hvis leverandøren bruker en databehandler (underleverandør) må de samme vilkårene i databehandleravtalen med kunden gjenspeiles i avtalen med den underleverandøren til leverandøren, for eksempel restriksjoner på bruk av underleverandører og overføring av personopplysninger utenfor EU. Leverandøren er ansvarlig for at underleverandører som benyttes, er forpliktet til å følge de samme vilkårene som er fastsatt i databehandleravtalen med kunden. Slik kan leverandørens kunder stole på at vilkårene som leverandøren har forpliktet seg til i kontrakten, også gjelder for andre selskaper som leverandøren samarbeider med for å levere tjenesten/produktet (underleverandørene).

Leverandøren må sørge for at de ansatte er kjent med pliktene i databehandleravtalen.

Ofte vil databehandleren ha mer kunnskap enn dataansvarlig om tjenesten som leveres. Det er derfor ofte lurt å ha god dialog mellom partene også før databehandleravtalen inngås.

6. Anbefalinger og krav til IKT og tekniske løsninger

6.1 Når blir et system å anse som medisinsk utstyr?

Leverandøren må vurdere om det som skal leveres blir å anse som Medisinsk utstyr. Ved tvil anbefales det å ta kontakt med Statens legemiddelverk. Det er egne regler for medisinsk utstyr.

Bruk av medisinsk utstyr i Helse- og omsorgssektoren reguleres av Forskrift om håndtering av medisinsk utstyr.

Les mer på Statens legemiddelsverks nettsider om medisinsk utstyr.

Se også Normens veileder for Medisinsk utstyr

6.2 Løsninger som benytter skytjenester

Normen sier at ved bruk av skytjenester for behandling av helse- og personopplysninger skal den dataansvarlige gjøre dekkende risikovurderinger, og ellers følger kravene til avtaler og leverandøroppfølging i Normen.

Kunden vil stille krav til den tekniske infrastrukturen som tjenesten kjører på. Normalt vil kunden etterspørre dokumentasjon på den tekniske løsningen, det kan være CAIQ eller tilsvarende dokumentasjon. Det stilles også egne krav til selve applikasjonen, og da spesielt til hvem som har tilgang til dataene, tilgangsstyring, logging.

Overføring av personopplysninger til andre land vil alltid være tema ved bruk av skytjenester. Som leverandør skal du kunne gi kunden oversikt over hvor dataene er lagret og fra hvilke land det gis tilgang.

Mer om sky kan du finne i Normens Veileder i bruk av skytjenester til behandling av helse- og personopplysninger. Mer om CAIQ kan du finne på https://cloudsecurityalliance.org/blog/2021/09/01/what-is-caiq/

6.3 Særlig om systemer som behandler helse- og personopplysninger

Når utstyr eller systemer behandler helse- og personopplysninger stilles det en rekke krav til håndtering av helse- og personopplysninger. I de tilfellene helse- og personopplysninger lagres i et system, blir det ofte ansett som et behandlingsrettet helseregister eller et fagsystem.

Behandlingsrettet helseregister er definert i Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) § 2 “pasientjournal- og informasjonssystem eller annet register, fortegnelse eller lignende, der helseopplysninger er lagret systematisk, slik at opplysninger om den enkelte kan finnes igjen, og som skal gi grunnlag for helsehjelp eller administrasjon av helsehjelp til enkeltpersoner”

Behandlingsrettede helseregistre skal være lette å bruke og å finne frem i og de skal være utformet og organisert slik at lovkrav kan oppfylles. Dette gjelder blant annet regler om

- taushetsplikt,
- forbud mot urettmessig tilegnelse av helseopplysninger
- retten til å motsette seg behandling av helseopplysninger
- retten til informasjon og innsyn
- helsepersonells dokumentasjonsplikt,
- tilgjengeliggjøring av helseopplysninger
- informasjonssikkerhet og internkontroll

Litt om tilgangsstyring

For å sikre at uvedkommende ikke får tilgang til helse- og personopplysninger, er det viktig at systemer har løsning for autentisering og autorisering

De fleste kunder har IAM-løsninger, som kan integreres mot. IAM står for Identity and Access Management, og det er en teknologi som brukes til å administrere og kontrollere tilgang.

Ved å integrere mot kundenes IAM-løsninger, kan man dra nytte av allerede etablerte sikkerhets- og identitetsstyringsprosesser. Man unngår prosesser som ofte manuelle og tidkrevende, i tillegg sikrer at hvem som har tilgang er oppdatert. Det anbefales at man benytter seg av IAM-løsningene når det er mulig.

Les mer om tilgangsstyring i Normens veileder for tilgang og faktaark for tilgangsstyring

Litt om logging

For å redusere risikoen for uautorisert tilgang helse- og personopplysninger er et av tiltakene logging. Når helseopplysninger aksesseres, skal tilgangen loggføres.

Det anbefales at systemer settes opp på en slik måte at logger blir tilgjengelig for logganalyseverktøyer som kunden har i bruk i sin organisasjon. Flere kunder har automatiske løsninger for analyse av logger.

Loggen skal oppbevares til det forventes å ikke lengre antas være bruk for den, og deretter slettes.

Les mer om logging i Normens faktaark for logging

6.4 Sikkerhetskrav til programmeringsgrensesnitt

Mye utstyr og systemer er satt opp for å utveksle opplysninger, enten det er ansattopplysninger for autentisering eller helseopplysninger som sendes mellom fag- og journalsystemer. Det er viktig at opplysningene beskyttes under «transport» mellom systemene, slik at det ikke er mulig å avlytte eller endre dataene. «Dørene» som opplysningene går inn/ut av, ofte referert til som API, må beskyttes ved pålogging eller andre sikkerhetstiltak for å hindre misbruk fra angripere. Et effektitv sikkerhetstiltak for å unngå avlytting eller endring av data er kryptering. Ifølge Normens kapittel 5.3.5 om Kryptering, bør all kommunikasjon sikres med kryptering, enten det skjer via trådløs kommunikasjon eller linjebaserte løsninger. Det bør også vurderes om dataene som er i «hvile» bør krypteres.

Det er ofte krav til hvilken protokoll som brukes og hvilke sikkerhetsmekanismer som er tilgjengelige. Innen helse- og omsorgssektoren brukes vanligvis HL7 2.x, FHIR eller DICOM for utveksling av medisinske opplysninger. DICOM er et meldingsformat med begrenset innebygd sikkerhet, derfor må det ofte legges til egne sikkerhetstiltak ved meldingsutveksling, spesielt når kommunikasjonen skjer over usikrede eller åpne nettverk.

Åpne API-er kan være lett å utnytte for en angriper, for eksempel ved å hente ut data eller brukes som et springbrett videre inn i organisasjonen. Det anbefales å benytte autentiseringsmetoder på API-er som settes opp, i tillegg til logging av trafikken.

Risikovurderingen bør inkludere integrasjoner. Risikomomenter som bør inngår i vurderinger, er:

- Sikre at data ikke kommer på avveie.
- Sikre at data kommer frem til mottaker. Man bør vurdere om det bør settes opp logging, med varsling når f.eks. en melding ikke kommer frem til mottaker.

6.5 Utprøving og utlån av utstyr

Ofte har helse- og omsorgstjenesten behov for å låne eller leie utstyr, enten det er i forbindelse med utprøving i en innkjøpsprosess eller for å møte økt behov eller behov for andre typer utstyr og løsninger som ikke er tilgjengelige for kunden. Ved utlån av utstyr er det nødvendig å avklare med kunden hvem som har ansvaret for konfigurasjonen. Dette kan omfatter alarmgrenser, brukeroppsett og integrasjoner, som må tilpasses kundens spesifikke behov og ønsker.

Hvis utstyret eller løsningen behandler helse- og personopplysninger, er det viktig at disse opplysningene kan slettes før utstyret eller løsningen returneres til leverandøren. Før utprøvingen eller utlånet starter, bør man vurdere om det er mulig å slette opplysningene på en godkjent måte. Hvis ikke, bør man vurdere å benytte pseudonymiserte opplysninger hvis dette er mulig.

6.6 Sletting av opplysninger

Normen og lovverket stiller krav om at virksomheten oppbevarer helse- og personopplysninger så lenge det er nødvendig for å oppnå formålene med behandlingen av opplysningene. Med mindre opplysningene deretter skal oppbevares i henhold til nye og legitime formål, skal opplysningene slettes eller anonymiseres.

For leverandører som behandler helse- og personopplysninger på vegne av kunden, enten som databehandler eller på annen måte, er det viktig å slette opplysninger som er lagret på en forsvarlig måte. Det er nødvendig å avtale rutiner for sletting med kunden og presentere en detaljert beskrivelse av hvordan slettingen gjennomføres. Beskrivelsen bør inneholde informasjon om både teknisk utførelse av slettingen og en tidsplan. I noen tilfeller kan det ikke være mulig å utføre slettingen umiddelbart etter at oppdraget er fullført. Det er derfor viktig å avtale dette med kunden og oppdatere databehandleravtalen. Dokumentasjon på at opplysningene er slettet, bør legges frem for kunden.

Eventuelle utskrifter og kopier skal makuleres eller slettes etter bruk. Slettingen skal utføres på en forsvarlig måte, og en metode skal brukes som forhindrer rekonstruksjon av opplysningene på en slik måte at den registrerte kan identifiseres. Begrensning av tilgangen til opplysningene ved hjelp av tilgangsstyring er ikke tilstrekkelig. For å oppfylle sletteplikten må virksomheten slette alle kopier av opplysningene, inkludert filer og data i sikkerhetskopier.

Hvis en dataansvarlig helsevirksomhet har benyttet seg av en databehandler for behandling av opplysninger, skal den dataansvarlige motta skriftlig bekreftelse på at alle helse- og personopplysninger er slettet etter at formålet er oppnådd. Dette skal reguleres i en databehandleravtale.

Les mer om lagring og sletting i Normens faktaark om lagringstid og sletting og i Nomens Veileder for rettigheter ved behandling av helse og personopplysninger

7. Anbefalte tiltak i forbindelse med etablering av nye systemer og oppgradering/migrering av eksisterende systemer

I helse- og omsorgssektoren er det stor avhengighet av teknologi for å kunne yte forsvarlig helsehjelp. Når utstyr og systemer kobles i nettverk, enten for å kommunisere internt i virksomheten mot andre systemer eller for å nå tjenester på internett, setter dette store krav til IT-sikkerhet. Det er viktig at utstyr og programvare er motstandsdyktige mot skadevare og hacking for å oppnå god sikkerhet og sikre at systemer fungerer i henhold til forventninger. For å kunne oppnå og opprettholde denne motstandsdyktigheten over tid, er det viktig at systemer, utstyr og programvare lar seg oppdatere på en sikker og kontrollert måte, enten det er firmware, sikkerhetspatcher eller programvareoppgraderinger. I de tilfeller der det er systemer som ikke lar seg oppdatere, og man derfor må benytte utstyr eller systemer med kjente sårbarheter, er det viktig å innføre sikkerhetstiltak, slik at man reduserer risikoen for at sårbarheter lar seg utnytte av virus eller hackere. Sikkerhetstiltak kan være både av teknisk art, som for eksempel segmentering av nettverk, herding av OS og fysiske tiltak, som å fysisk hindre tilgang til USB-porter.

Ledelsen hos kunden har ansvaret for å sikre at etablering av nye systemer og oppgradering/migrering av eksisterende systemer ikke innebærer risiko for behandling av helse- og personopplysninger og ytelsen av helsehjelp. Dette ansvaret inkluderer gjennomføring av kontroll, vurdering av risiko, planlegging for helsehjelp uten IKT (systemstøtte) og grundig testing før de nye systemene tas i bruk. Leverandøren av de nye systemene vil ofte være ansvarlig for den IT-tekniske konverteringen og oppstarten av systemene. En god forståelse mellom kunden (som er ansvarlig for databehandling) og leverandøren er avgjørende for et vellykket resultat.

Videre i dette kapittelet beskrives viktige aktiviteter som virksomheten bør gjennomføre i samarbeid med leverandøren. Rekkefølgen av punktene kan variere avhengig av prosesstypen, enten det er innføring av et nytt system, konvertering eller bytte.

Som støttedokument til veilederen følger et flytskjema som beskriver de viktigste stegene i et konvertering- og innføringsløp. Dette flytskjemaet viser en naturlig rekkefølge mellom de ulike stegene. I praksis vil det imidlertid ofte være slik at man hopper frem og tilbake mellom stegene i flytskjemaet. Smidig metodikk er en måte å organisere og gjennomføre prosjekter/utvikling på som gir rom for stadig forbedringer og endringer. Dersom innføringen benytter smidige metoder vil både utvikling, testing og innføring kunne skje i kortere iterasjoner, slik at systemet utvikles og innføres gradvis. Dermed vil flere av stegene i flytskjemaet gjøres for kun deler av systemet om gangen, for så å gjentas for hver videreutvikling av systemet.

Risikovurdering

For å sikre at prosessen ikke medfører unødige risikoer, er det viktig at det gjennomføres en risikovurdering. Det er kunden som er ansvarlig for at vurderingen gjennomføres. Leverandøren bør bistå kunden i gjennomføring av risikovurderingen. Risikovurderingen bør oppdateres hvis risikobildet endres i løpet av innføringsprosessen.

Vurderingen bør blant annet inkludere:

- mulig nedetid vil ikke påvirke evnen til å yte forsvarlig helsehjelp
- feil med konvertering, slik at data blir utilgjengelig eller feil
- tilgjengelig kompetanse, både teknisk og klinisk
- tekniske risikoer; nettverksproblematikk, brannmur, skalerbarhet av nytt produksjonsmiljø
- prosessen med konvertering av data. Er det data som ikke blir konvertert, eller er det kjente begrensninger i hvilke data som lar seg konvertere.

Gjennomføre møte med involverte parter og planlegg innføring (oppstartsmøte)

Leverandøren bør utarbeide en beskrives hvordan innføring og eventuell konvertering blir gjennomført. For nye systemer som skal erstatte eksisterende systemer, samt oppdateringer som medfører endre funksjonalitet, bør det kartlegges hva som er av endringer. Brukermanualer og prosedyrer bør oppdateres i god tid før planlagt oppstart/konvertering, slik at sluttbrukere er godt kjent med endringer. Det er leverandørens ansvar for at brukermanualer er oppdatert. Prosedyrer er kundens ansvar, men leverandøren bør bistå kunden.

Ansvarsklargjøring og avtaler

Det må avklares hvem som er ansvarlig for hvilke delprosesser under innføringsprosessen. Ansvarsfordelingen bør avklares i god tid før innføring og dokumenteres. En HUKI-Matrise er et godt verktøy for å plassere ansvar i forbindelse med innføring og konverteringsprosesser. Det er flere som har god erfaring med bruk av HUKI også i driftsfasen. Eksempel på en HUKI-Matrise er støttedokument til denne veilederen.

Det anbefales det opprette en avtale mellom leverandør og kunde som bør inneholde følgende:

- tidspunkt for konvertering og bytte
- bekreftelse for tidspunktene 2 dager før planlagt dato
- ansvar for kontroll av konverterte data slik at de enkelte delene er korrekt konvertert
- gjennomføring av veiledning og opplæring i den nye løsningen
- hvem som skal kontaktes ved problemer og spørsmål, både hos leverandør og kunde. Samt tidspunkt når støttepersonell skal være tilgjengelig
- forsterket support de nærmeste dagene etter konvertering. Helst direktenummer til en navngitt person som kan følge opp tettere enn brukerstøtte

Forberede innføring, konvertering og bytte

Kunde er ansvarlig for å avklare tidspunkt som er gunstig å gjennomføre innføring, konvertering og bytte med berørte parter.

Leverandør oppfordres til å oppgi referanser hvor tilsvarende innføring-, konvertering- og bytteprosesser leverandøren har gjennomført.

Utarbeide tids- og ressursplan

Det anbefales at det utarbeides en tids- og ressursplan, som alle parter er omforen om, og som er godt forankret hos sluttbrukere.

Utarbeid testprotokoller og akseptkriterier

Det må utarbeides tester som skal gjennomføres for å kontrollere at konvertering og bytte er gjennomført korrekt.

Eksempler er at antall journaler i ny EPJ er likt antall journaler i gammel EPJ, åpne og sjekke innhold i journaler ift innhold før konvertering og bytte

Plukk ut et utvalg journaler for kontroll, antallet bør være høyt nok til å kunne avdekke eventuelle feil.

Kartlegge driftsmiljøet

Kundens driftsmiljø bør kartlegges, eventuelt sammen med kundens IT-leverandør, og det bør utarbeides en tilstandsrapport. Leverandøren kan levere retningslinjer for hvordan kartleggingen skal gjøres og kan bistå kunden om nødvendig. Med driftsmiljø menes maskiner, programmer og nettverk med oppsett.

Det anbefales å vurdere om det er behov for opprettelse av dedikerte miljøer for test og pro-test.

Endringer i maskinvare (Utarbeide teknisk tilstandsrapport og Bestilling av eventuelle endringer)

I de tilfellene klarleggingen avdekker behov for endringer i utstyr og maskinvare, som er nødvendig i forbindelse med innføring av nye systemer og/eller konvertere av eksisterende systemer. Må leverandøren gjøre kunden oppmerksom på dette, slik at kunden kan anskaffe nytt utstyr, eller foreta nødvendige endringer i god tid.

Det er viktig at alle deler av systemet er tester før man går i produksjon. Hvis det er kritiske systemer, bør man vurdere å gjennomføre en «prod-test» før man går i produksjon. Dette for å sikre at alt fungerer som det skal (pålogging, integrasjoner, passord). Prod-test bør inkludere sluttbrukere. Det anbefales det opprettes en test-protokoll som beskriver hva som skal testes og hvem som er ansvarlig. Ofte har kunden maler på slike protokoller tilgjengelig.

Informasjon til andre berørte parter

Hvis innføring/konvertering påvirker andre deler av organisasjonen hos kunden eller kundens samarbeidsparter, er det viktig at disse blir orienter på planlagt aktivitet og tidsplan. Det anbefales at det setts opp en oversikt og sjekk at alle berørte parter er informert. Med berørte parter menes alle som deltar eller blir påvirket av prosessen.

Gjennomfør opplæring i nytt system

Den som er ansvarlig skal blant annet

- oppdatere brukerdokumentasjonen
- opprett alle brukere med korrekt rolle og tilgang
- gjennomfør opplæring i det nye systemet
- opplæringen skal være tilstrekkelig slik at helsepersonell er kjent med funksjonalitet som er nødvendig for å utføre pålagte oppgaver

Gjennomfør prøvekonvertering – akseptansetest

Ved migrering av systemer anbefales det å gjennomføre prøvekonvertering slik at tekniske utfordringer oppdages på forhånd.

Prøvekonvertering må skje i god tid før planlagt konvertering.

Etter at prøvekonvertering er gjort, er det viktig at data som er konverter blir analysert, for å avdekke eventuelle feil i forbindelse med konvertering. Det er viktig at sluttbruker involveres i analysen, da de ofte er de som kjenner best til dataen, og kan avdekke eventuelle feil. Hvis det oppdages feil, bør prøvekonvertering gjentas til man oppnår ønsket resultat.

Konvertering av eksisterende løsninger

Leverandøren bør beskrive om konverteringen skal bruke ferdige konverteringsprogrammer som er testet og benyttet tidligere, eller om det må utarbeides egne konverteringsprogrammer for denne konverteringen

Alle involverte parter (leverandør, sluttbrukere, teknisk) bør gå gjennom konverteringen slik at alle parter er enige og forstår hva som skjer i konvertering og bytte.

Ved bruk av egne konverteringsprogrammer er det særskilt viktig at helsepersonell og leverandør er enige om og forstår hvilke endringer som vil bli gjennomført. Det er økt risiko for feil når det utvikles egne konverteringsprogrammer for konvertering

Hvis konvertering gjøre i leverandørens infrastruktur, er det viktig at dette inngår i en databehandleravtale. Og at opplysninger slettes etter at konvertering er ferdig.

Avslutte eksisterende løsning

Henvisninger og meldinger som ligger i det gamle systemet må sendes før det avsluttes, slik at meldinger ikke blir «borte».

Gjennomfør konvertering og bytte

Leverandøren bør utføre konvertering i samarbeid med kunden.

Forbered ytelse av helsehjelp

Det må lages gode planer for drift uten systemstøtte i den planlagte tiden konvertering og bytte er planlagt. Planlegg ekstra nedetid uten tilgang til systemet for sikkerhets skyld.

Alternativt planlegg med å stenge ytelse av helsehjelp til konverteringen og bytte er utført

Akseptansetest

Tester utføres iht. testprotokoll. Oppdages det feil skal konverteringen gjennomføres på nytt, og samtlige tester gjentas. Denne prosessen må gjentas frem til man oppnår ønsket resultat.

Når akseptansetest er gjennomført og godkjent, signeres protokollen av både leverandør og helsepersonell som kvittering på at testene er gjennomført og innholdet er korrekt

Klargjør for å ta i bruk nytt system

De som har hatt ansvar for sikkerhetskopier, arkiver de på et trygt sted. Og sikrer for sletting av disse, når formålet er oppnådd.

Kunde bør utarbeid et dokument som signeres av helsepersonell og leverandør, som bekrefter at opplæringen er gjennomført og helsepersonellet er kjent med nye systemet

8. Lokalt installert programvare/systemer hos kunden

Det er mange systemer og løsninger som installeres og kjøres lokalt hos kunden. Det kan være utfordrende og holder slike systemer oppdatert. Ofte er det manuelle prosesser som krever fysisk tilgang, og i mange tilfeller håndteres dette av de som har driftsansvaret lokalt. For slike systemer er det viktig å gjennomføre fortløpende vurderinger av sikkerheten i og rundt denne typen utstyr og systemer. Både trusselbildet og mulighetsrommet endrer seg kontinuerlig, og det som var trygt å bruke den ene dagen kan være usikkert og utgjøre en trussel den neste dagen. Den programvaren/systemet som ikke lot seg oppdatere, kan ha fått tilgjengelig oppdateringer som bidrar til økt sikkerhet. God kommunikasjon mellom kunde, leverandør og produsent er viktig for å kunne holde systemene oppdatert og sikre god IT-sikkerhet.

Eksempler på lokalinstallerte systemer:

- styring av heis
- adgangssystem
- styringssystemer for strøm, vann og ventilasjon.
- medisinsk utstyr
- lokalt installerte servere
- lokalt installert programvare

Noen av systemene behandler ikke helse- og personopplysninger, men virksomhetene er ofte avhengige av disse systemene for å kunne yte forsvarlig helsehjelp. Det er også ofte systemer som er integrert med andre systemer eller kommuniserer i samme nettverk. Tradisjonelt sett er dette systemer med lav modenhet når det kommer til grunnleggende IT-sikkerhet. Ofte mangler det en systematisk tilnærming til sikkerhetsoppdateringer, og det kan være utdaterte versjoner av operativsystem. I noen tilfeller vil det ikke være mulig å foreta oppdateringer, slik at utdaterte versjoner må benyttes.

Medisinsk utstyr og OT er systemer som ofte består av komplekse nettverk med underliggende komponenter som har utdaterte eller proprietære operativsystemer. Det er viktig at disse systemene beskyttes på en god måte, både for deres egen sikkerhet, men også for at disse systemene ikke skal utgjøre en trussel for andre deler av virksomheten. Som leverandører av slike systemer bør man tilby løsninger som lar seg oppdatere og sikkerhetspatche. Man bør jobbe for å holde systemene oppdatert, både når det kommer til sikkerhetspatcher og oppdateringer av operativsystem. Normen sier at systemer skal være robuste, og det er viktig at leverandører av slike systemer bistår kunden på best mulig måte, slik at både systemet og omkringliggende systemer blir robuste og sikre. Typiske tiltak kan være å bistå med råd om hvordan systemet kan settes opp for å ivareta krav til robusthet og sikkerhet, som for eksempel brannmur, segmentering av nettverk og antivirus.

9. Utstyr plassert hjemme hos pasient/bruker

Når pasienter får utstyr og løsninger for digital hjemmeoppfølging i helsesektoren, er det viktig at disse systemene støtter sikker og trygg yting av helsehjelp. Ved implementering av slike løsninger må man ta hensyn til at pasientens hjem kan ha ulike sikkerhetsutfordringer sammenlignet med et sykehus eller sykehjem. Det kan også være brukere som mangler kunnskap om hvordan teknologien skal brukes. Det er derfor viktig å gjennomføre en risikovurdering før teknologien tas i bruk. Eksempler på risikoer inkluderer:

- ustabil nettverksforbindelse (bredbånd og mobilnett)
- usikker strømforsyning
- mulig uautorisert tilgang til utstyret, som kan føre til uønskede endringer, for eksempel endring av alarmgrenser
- manglende forståelse eller adekvat håndtering av alarmer fra brukeren, som for eksempel batteribytte i trygghetsalarm

- er teknologien egnet for pasientgruppen den er tiltenkt
- manglende tilgjengelighet av opplysninger for helsepersonell

Mye av utstyret og systemene i pasientens hjem er designet for å sende data fra pasienten til helsetjenesten (enveis kommunikasjon). Utviklingen går nå mot toveis kommunikasjon der utstyr kan både sende og motta data, kommunisere med brukeren via tekst, lyd eller bilde, og i visse tilfeller endre innstillingene på utstyret eksternt uten fysisk tilgang til utstyret eller brukeren.

For løsninger der behandlingen kan endres via skytjenester eller internett, bør det gjennomføres en grundig risikovurdering. Eksempler på risikoer inkluderer:

- Tilgangskontroll, som kan være problematisk med skytjenester på grunn av manglende integrasjon med kundens ansattregister (IAM-løsning). Dette kan føre til at tidligere ansatte eller personer som har byttet stilling fortsatt har tilgang.
- Sikker identifisering av pasienten. Pseudonymisering av pasienten er et vanlig sikkerhetstiltak, men det kan påvirke pasientsikkerheten negativt. Prosessen med re-identifisering av pasient/bruker er ofte en manuell prosess, og øker risikoen for forveksling.

Les mer om sky i Veileder i bruk av skytjenester til behandling av helse- og personopplysninger , om medisinsk utstyr Veileder i personvern og informasjonssikkerhet - medisinsk utstyr og om velferdsteknologi i Veileder i informasjonssikkerhet og personvern ved bruk av teknologi i kommuner (velferdsteknologi).

10. Tilgang til utstyr plassert hos kunden

10.1Fjernaksess

I mange tilfeller trenger leverandøren tilgang til kundens systemer og utstyr for å kunne gi støtte og håndtere feil. Det er også vanlig at mye utstyr og systemer oppdateres ved hjelp av fjernaksessløsninger eller har "Call-home"-funksjon. Utstyr med "call-home" er ofte store installasjoner som CT, MR og PET, som sender teknisk status tilbake til fabrikken. Dette bidrar til å rette feil på utstyret før de utvikler seg til alvorlige problemer som krever nedetid for utstyret. Det finnes også utstyr og systemer som automatisk henter oppdateringer fra produsentens servere på internett. Dette kan inkludere oppdateringer og patcher både for selve produktet og operativsystemet. Disse løsningene kan sammenlignes med Windows Server Update Services (WSUS).

Innen sektoren er det mange forskjellige fjernaksessløsninger tilgjengelig, og mange kunder krever at leverandøren bruker deres spesifikke løsning. Dette kan noen ganger være i konflikt med kravene, for eksempel når det gjelder 24/7-365 support. I slike tilfeller kan det være nyttig å ha en dialog med kunden for å finne en løsning som tilfredsstiller begge parter. Ofte skyldes kravet om bruk av kundens løsning bekymringer for sikkerhet og usikkerhet om hvorvidt leverandørens løsning vil ivareta sikkerheten tilstrekkelig. Det er derfor viktig å ha

god dokumentasjon og gi kunden innsyn i løsningen, samt tilby muligheten for revisjoner hvis ønskelig.

Fjernaksessløsninger bør inkluderes i risikovurderingen, som skal omfatte både teknisk sikkerhet og pasientsikkerhet.

Eksempel:

Et akuttsykehus har kun en MR-maskin, den er koblet opp mot produsenten med fjernaksess. Maskinen rapporterer teknisk status tilbake til fabrikken, og servicepersonell hos produsenten/leverandøren kan aksessere maskinen for å undersøke eventuelle feil. Feil vil kunne oppdages tidlig og før det medfører driftsavbrudd. Større feilretting vil kunne gjennomføres kontrollert, slik at man kan sende akuttpasienter til et annet sykehus. Hvis man velger å ikke tillate denne type kommunikasjon, kan dette påvirke pasientsikkerheten negativt.

Norsk Helsenett har egen fjernaksessløsning som er tilgjengelig for de som er koblet til NHN.

Les mer om Fjernaksess i Veileder for fjernaksess mellom virksomhet og leverandør

10.2 Reparasjon og service på utstyr plassert hos kunden.

Når leverandøren utfører reparasjon og service på utstyr som er plassert hos kunden, får de ofte tilgang til infrastruktur og lokasjoner som normalt er forbeholdt kundens eget personell.

Som leverandør er det viktig å sette seg inn i kundens rutiner, for eksempel virusvasking av minnepinner og andre flyttbare lagringsmedier som skal brukes i forbindelse med service og reparasjon. Det er viktig å være forsiktig og alltid avklare om de ønskede aktivitetene kan utføres uten å påvirke eller utgjøre en fare for andre systemer hos kunden. Dette kan inkludere å stoppe en server, koble fra en nettverkskabel eller slå av et apparat.

Det er også viktig å være oppmerksom på områder hvor man ikke skal eller bør oppholde seg. Innen helsesektoren er det spesielle krav til arbeidsområder, enten det dreier seg om smittevern, nukleære områder (strålevern) eller områder med strømforsyning. Leverandører som arbeider hos kunden, må ha nødvendige kurs og sertifiseringer eller be om at noen fra kundens personell følger med for å sikre at arbeidet blir utført på en trygg og sikker måte. Typiske kurs kan inkludere FSE (Forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg) og strålevern.

10.3 Håndtering av utstyr mottatt fra kunden for service\reparasjon\destruksjon som inneholder personopplysninger

Når utstyr mottas fra kunden og dette utstyret inneholder helse- og personopplysninger, er det viktig at disse opplysningene håndteres på en sikker måte. Det er viktig å begrense hvem som får tilgang til opplysningene, og sikre at de som får tilgang er kjent med taushetsplikten.

Hvis utstyr skal kasseres/destrueres, skal opplysninger som er lagret på utstyrets lagringsmedier slettes. Lagringsmedier bør destrueres på en sikker måte.

Les mer om lagring og sletting i Normens faktaark om lagringstid og sletting.

11. Normens krav i anskaffelser

Helsepersonell er helt avhengige av, og prisgitt ulike IT-verktøy og systemer for å yte forsvarlig helsehjelp. Løsninger og systemene må være tilrettelagt for god informasjonsflyt innad i virksomheter, og mellom ulike virksomheter og nivåer i helsetjenesten.

Alle Normens krav er utledet fra lovkrav og inneholder totalt 294 «skal-krav» som detaljerer og supplerer lovkrav. Ikke alle disse kravene er relevante i forbindelse med anskaffelser.

I anskaffelsesprosesser er det vanlig at det stilles krav til at løsningen skal oppfylle Normen, eller at leverandøren skal følge Normen. Dette kan imidlertid være vanskelig å evaluere for kunden og skape et dårlig grunnlag for en kontrakt. For å kunne evaluere dette på en god måte og danne det beste grunnlaget for kontrakten, er det viktig at både leverandør og kunden har god kommunikasjon og kjennskap til kravene. Dette bidrar til å sikre at begge parter har en felles forståelse og forventninger til hva som kreves, og det øker sannsynligheten for en vellykket kontrakt og et godt samarbeid mellom partene.

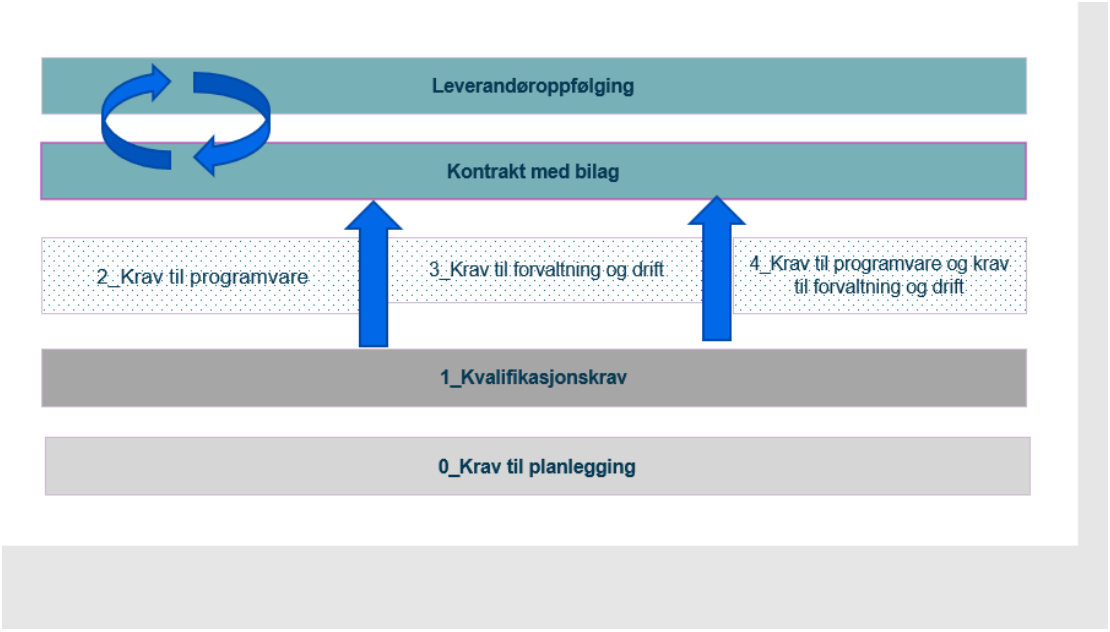
For å kunne vurdere om et system skal tas i bruk, må risiko for informasjonssikkerhet, personvern og pasientsikkerhet vurderes. Det er ledelsens ansvar i hver enkelt virksomhet å vurdere om risikoene ved å implementere et system er akseptable eller ikke. Grundige risiko- og personvernvurderinger vil kunne bidra til en bedre forståelse av disse risikoene og styrke beslutningsgrunnlaget for ledelsen.

Dokumentet «Hvordan bruke Normens krav i anskaffelser» (excelliste) er et støttedokument som kan benyttes i forbindelse med anskaffelser for både oppdragsgiver og leverandør. Målet er å gjøre det lettere å bruke Normens krav i anskaffelser. Det er en forutsetning at de som bruker plukklisten har kompetanse til å vurdere hvilke krav som er relevante for den aktuelle anskaffelsen. Excellisten kan brukes som en plukkliste med krav som gir støtte i arbeidet med konkurransegrunnlag, utarbeidelse av kvalifikasjonskrav og kravspesifikasjoner. Dokumentet inneholder også mapping av alle Normens krav mot krav i NS-EN ISO/IEC 27001:2017og NS-EN ISO/IEC 27002:2017. Det er også et laget et dokument som gir veiledning til hvordan dette kan brukes.

Excellista og veiledning finner på på normen.no under Oversikt over Normens krav og mapping mellom ISO, CCM og Normen

Krav i Normen som er aktuelle er delt inn i

- Krav til planlegging
- Kvalifikasjonskrav
- Krav til programvare
- Krav til forvaltning og drift
- Krav til programvare og krav til forvaltning og drift



Etter gjennomført anskaffelsesprosess og inngåelse av kontrakt (-er) vil konktrakt med tilhørende bilag være grunnlag for oppdragsgivers tilgang til tjenester fra leverandør og plikt til oppfølging av leverandør.

12. Om Norsk Helsenett

Som leverandør til kunder som er tilknyttet NHN, er det mulig for deg som leverandør å benytte tjenester som tilbys av NHN. Eller selv og knytte deg til NHN.

«Norsk Helsenett SF skal sørge for at det foreligger en hensiktsmessig og sikker infrastruktur for effektiv samhandling mellom alle deler av helse- og omsorgstjenestene, og bidra til forenkling, effektivisering og kvalitetssikring av elektroniske tjenester til beste for pasienter og befolkningen for øvrig».

«Foretaket skal sørge for nødvendig samordning av infrastrukturtjenestene i helsesektoren og understøtte god kommunikasjon mellom aktørene i helsetjenesten.»

- **Helsenettet** driftes og forvaltes av Norsk helsenett. Helsenettet er et medlemsnettverk og et verdinettverk for samhandling i helsesektoren. Her kan sykehus, apotek, fastleger og andre som yter helsetjenester kommunisere og utveksle helseopplysninger på en trygg og lovlig måte. Helsenettet ivaretar sikkerheten slik at næringslivet kan tilby sin teknologi/sine tjenester til helsesektoren
- **Nasjonale e helse løsninger** som driftes og forvaltes av Norsk helsenett er: Helsenorge, E-resept, Kjernejournal
- **Mange ulike registrere og samhandlingstjenester** driftes og forvaltes av Norsk helsenett

NHN ønsker å være et informasjons- og samhandlings nav i helse- og omsorgstjenesten. Med ansvar for et verdinettverk der de både skal gjøre det enkelt for medlemmene deres å

komme i gang med NHNs helsepersonelltjenester og strategi for at aktørene/leverandørene skal lettere kunne tilby sine tjenester og skape innovasjon på NHNs plattform.

Norsk Helsenetts skal legge til rette for at medlemmene av Helsenettet skal få tilgang til nyttige og relevante tjenester. Noen tjenester leverer NHN selv, mens andre leveres av leverandørene. Det er leverandørene som først og fremst skaper merverdi i Helsenettet. Derfor tilrettelegger NHN for en godkjenning av leverandører, slik at de kan få tilby sine tjenester til sektoren. Leverandøren blir da også medlem i Helsenettet. Leverandører som er medlemmer i Helsenettet er forpliktet til å følge kravene i Normen gjennom Tredjepartsavtalen og medlemsvilkårene.

Godkjenning av virksomheten- leverandøren, tilgang og oppkobling til Helsenettet og de ulike nasjonale e-helseløsningene gjøres for å:

- Ikke påføre eksisterende virksomheter i Helsenettet økt risiko ved å koble til nye virksomheter og tjenester.
- Verifisere at leverandør har dokumentert at tjenestene og løsningene blir levert og produsert i et miljø som lever opp til sektorens krav.

NHN har krav og retningslinjer i en slik godkjenning, som er beskrevet her: Tredjepartsleverandører i Helsenettet - Norsk helsenett (nhn.no)

Det er en forventning fra Norsk helsenett at leverandøren integrerer og tilrettelegger for de nasjonale e-helseløsningene og tjenestene

FJENERNSUPPORT – fjernaksess i Helsenettet

Norsk Helsenett tilbyr NHN fjernhjelp i Helsenettet. Denne løsningen krever at man er godkjent leverandør hos NHN, men har ikke krav om helsenett tilknytning

Denne tjenesten for fjernhjelp, vil ikke utløse noen ekstra kostnader for hverken sluttkunden eller for godkjente leverandører av fjernhjelp i Helsenettet. Altså en gratis medlemstjeneste.

Fjernhjelp gir leverandører tilgang til maskiner i Helsenettet for å gjennomføre support og driftsoppgaver, uten å være fysisk til stede hos kunden.

Med fjernhjelp kan leverandører i Helsenettet bistå sine kunder på en sikker og effektiv måte med brukerstøtte og/eller vedlikehold. Dette medfører at personalet i den enkelte virksomhet bruker mindre tid på å løse problemer og reduserer tid brukt på reising og veiledning.

Fjernhjelp - Norsk helsenett (nhn.no)

Vedlegg

Flytskjema innføringsprosessen

HUKI-Matrise