Direktoratet for e-helse

Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten

EI-1012

Publikasjonens tittel:
Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten

Rapportnummer
IE-1012

Utgitt:
Desember 2017

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Postadresse:
Postboks 6737 St. Olavs plass, 0130 OSLO

Besøksadresse:
Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70

Forord

Helse- og omsorgsdepartementet ga i juni 2017 Direktoratet for e-helse i oppdrag å gjennomgå informasjonssikkerheten ved bruk av private leverandører i helse- og omsorgssektoren (Tillegg til tildelingsbrev nr. 4, datert 09.06.2017) og levere en rapport innen 1. desember 2017.

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. I rapporten gis det en overordnet status for bruk av private IKT-leverandører innen helse- og omsorgs-sektoren, basert på den informasjon sektoren selv har frembragt.

I rapporten er det gitt forslag til kriterier og rutiner som kan danne grunnlag for det videre arbeidet med informasjonssikkerhet ved bruk av private leverandører. Forslagene bygger på innspill fra et bredt spekter av relevante aktører. Synspunkter på om det er tjenester som ikke bør settes ut og synspunkter på forholdet mellom helsetjenesten og sikkerhetslovgivning er omtalt i egne kapitler i rapporten.

Det gis videre anbefalinger for hvordan kravene til informasjonssikkerhet bedre kan etterleves, basert på fagkompetanse i Direktoratet for e-helse, innspill fra helse- og omsorgssektoren, kompetansemiljøer og IKT-leverandører til helse- og omsorgssektoren, samt fra fag- og pasientorganisasjoner. Informasjon er i tillegg hentet fra noen parallelle initiativer, pågående prosjekter og annet tilgjengeliggjort referansemateriale.

Rapporten er ikke en kontroll- eller tilsynsrapport. Den skal bidra til at person-vern og informasjonssikkerhet ivaretas, samtidig som leverandørsamarbeidet videreutvikles. Godt leverandørsamarbeid oppnås gjennom klarhet i hvilke forutsetninger som gjelder relatert til juridiske, avtalemessige og tekniske forhold.

Et stort antall aktører fra helse- og omsorgssektoren, kompetansemiljøer, fag- og pasientorganisasjoner og IKT-næringen har deltatt i prosessen. Det er også mottatt faglig nyttig innspill fra andre sektorer og vi takker Finanstilsynet, Telenor og Statoil for den informasjonen og erfaring de har delt med oss.

Vi takker alle deltagere for et stort engasjement, og spesielt de regionale helseforetakene. Vi anbefaler at dialogen videreføres med aktørene i det etterfølgende arbeidet.

Oslo, 1. desember 2017

Innhold

NAVIGASJON I RAPPORTEN: Tilbake til innholdssiden

1 Sammendrag

Denne rapporten er Direktoratet for e-helses svar på oppdrag fra Helse- og omsorgsdepartementet (HOD) om å gjennomgå informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgssektoren (Tillegg til tildelingsbrev nr. 4, datert 09.06.2017).

Helse- og omsorgssektoren har ambisiøse mål og store forventninger til modernisering og effektivisering. Digitalisering er et viktig hjelpemiddel for å nå disse målene og utviklingen på området går raskt. Sektoren er helt avhengig av private leverandører, både nasjonale og internasjonale, innen IKT-området, for å sikre tilgang til oppdatert teknologi, løsninger og tilstrekkelig kompetanse. Pasienter og innbyggere må ha tillit til at informasjon blir håndtert på en trygg måte. Pasientene forventer at både konfidensialitet, integritet og tilgjengelighet ivaretas. Sektoren må balansere disse til det beste for pasienten og i tråd med lovverket. Flere virksomheter i sektoren har komplekse og gamle løsninger. Dette medfører at arbeid med digitalisering og informasjonssikkerhet er krevende.

Status for bruk av private leverandører

Bruk av private leverandører varierer i dag mellom aktørene og ulike områder. De fleste aktørene drifter sine egne løsninger, bortsett fra fastlegene som bruker private leverandører til de fleste IKT-oppgaver. For applikasjonsforvaltning, -utvikling og -innføring får aktørene i stor grad bistand fra private leverandører, med noen få unntak. Medisinsk-teknisk utstyr leveres av private leverandører og disse utfører også support på utstyret. Skytjenester brukes i dag i veldig begrenset omfang, men det forventes at både tilbudet, behovet og ønsket om bruk av skyløsninger raskt vil øke. Private leverandørers ansatte vil i arbeidet få tjenestemessig nødvendig tilgang til pasientinformasjon.

Vurdering av om det er tjenester som ikke bør overlates til private leverandører

Direktoratet for e-helse mener at det ikke er grunnlag for å konkludere med at noen typer tjenester aldri kan overlates til private leverandører. I gjeldene rett er det ikke noe forbud mot at norske virksomheter benytter nasjonale eller utenlandske, private leverandører fra EU/EØS-området. Ved bruk av globale leverandører (utenfor EU/EØS) er det særskilte krav som må oppfylles.

Det må alltid foretas en risikovurdering av alle tjenester som kan gi tilgang til pasientinformasjon. Risikovurdering og varsling etter sikkerhetsloven § 29 a om kritisk infrastruktur må gjennomføres der det er relevant, og dette må vurderes ved større IKT-prosjekter. Direktoratet for e-helse mener at helse- og omsorgssektoren generelt må ha en relativt lav risikoappetitt. Tillit fra innbyggerne til at helse- og omsorgssektoren behandler helseopplysninger på en sikker måte, er en forutsetning for å lykkes med digitalisering.

Viktige tiltak og forbedringsområder

Det foreslås tiltak og forbedringsområder av to kategorier – tiltak og forbedringer virksomheter i sektoren selv må gjøre og tiltak som må følges opp sentralt. Sektoren består av både store og små virksomheter med ulike utfordringer for å tilpasse seg et felles regelverk. Foreslåtte tiltak er ikke nødvendigvis relevant for alle virksomheter i sektoren, og tiltakene må tilpasses den enkelte virksomhet.

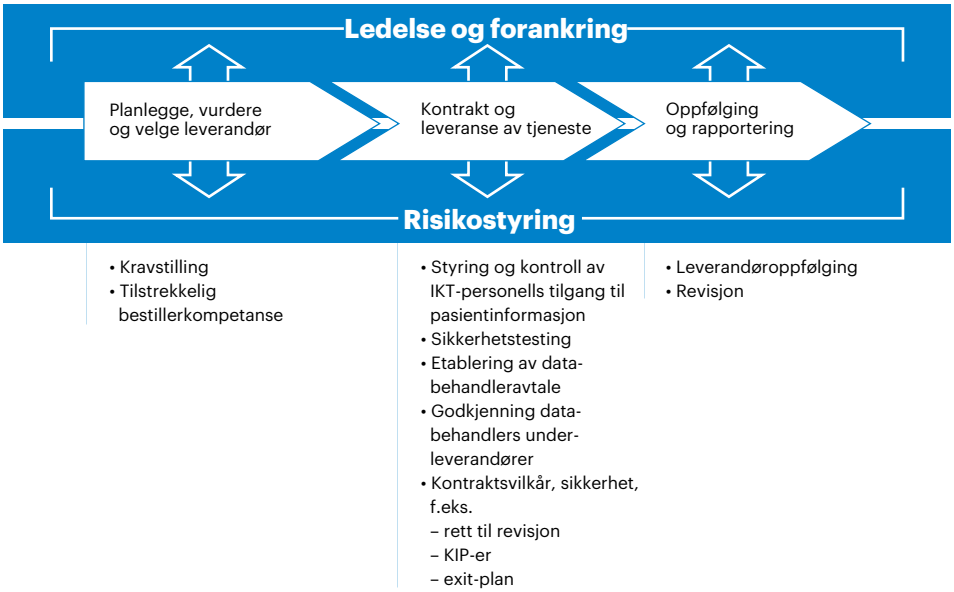
Tiltak og forbedringsområder for virksomhetene i sektoren

- **God og reell ledelsesforankring og styring**
  Virksomheten må ha en helhetlig styringsmodell med klarhet i ansvar og roller knyttet til informasjonssikkerhet, herunder forholdet til private leverandører. Det er behov for bedre ledelsesforankring. Dette må underbygges av gode prosesser som anvendes aktivt i den totale virksomhetsstyringen.

- **Helhetlig risikovurdering**
  Når tjenester overlates til private leverandører må det foretas en helhetlig risikovurdering slik at den totale risikoen kommer frem og rapporteres til ledelsen. Risikovurdering og tiltak må ta høyde for de begrensinger som finnes i nåværende, eldre og komplekse tekniske løsninger. Det er viktig med både periodisk oppfølging og nye risikovurderinger når det gjøres endringer i tjenesten eller leveransestrukturen. Nødvendige risikodempende tiltak må ha tilstrekkelig finansiering.

- **Behov for kompetanse**
  Virksomheten må ha tilstrekkelig kompetanse, kapasitet og struktur for å ivareta sitt ansvar for informasjonssikkerhet og personvern når private leverandører benyttes. Bestillerkompetansen må være god i alle faser, fra kravstilling i planleggings- og anskaffelsesfasen til leverandøroppfølging i driftsfasen. Ledelsen, inkludert styret, må ha tilstrekkelig kompetanse for å utøve reelle styring og kontroll også på dette området.

Det er foreslått en rekke kriterier og rutiner som bør følges for å sikre pasientinformasjon ved bruk av private leverandører. Noen sentrale kriterier og rutiner som rapporten peker på er:



Tiltak og forbedringsområder som må gjennomføres sentralt

- **Avklaring av databehandlingsansvar mellom regionale helseforetak og helseforetak**
  Databehandlingsansvaret ligger i dag på den enkelte virksomhet, som for eksempel et helseforetak. Dette skaper uklarhet i styring og ansvar ved anskaffelser og innføring av regionale løsninger og ved løsninger på tvers av sektoren.

  Det må utredes om databehandlingsansvaret slik det er i dag er forenlig med strategier for etablering av fellesløsninger i helse- og omsorgssektoren. Det bør særskilt vurderes om det er behov for regulering av felles databehandlingsansvar eller fordeling av dette ansvaret mellom regionale helseforetak og helseforetakene de eier.

  Det er viktig å få gjennomført dette arbeidet så raskt som mulig, da dagens kompliserte ansvarsforhold påvirker og forsinker arbeidet med digitalisering i helse- og omsorgssektoren.

- **Oppdatering av Normen**
  Følgende oppdateringer av Norm for informasjonssikkerhet i helse- og omsorgstjenesten må prioriteres for at Normen kan bli et bedre verktøy tilpasset alle brukergruppene:
  - *Tilpasning til GDPR (pågår)*
  - *Oppdatere rutiner og maler for å understøtte komplekse leverandørstrukturer og leveransmodeller (erfaring andre sektorer)*
  - *Rutiner for helthetlig risikostyring*
  - *Nasjonal standard for tilgangsstyring (private leverandører)*
  - *Standardiserte databehandleravtaler*

- **Kompetanseheving innen IKT-sikkerhet og risikovurdering på styre- og ledelsesnivå**
  Det anbefales etablering av et forum for beste praksis i bransjen for kompetanseheving innen områder som IKT-sikkerhet, risikovurdering og sikkerhetskultur.

- **Øvrige funn for oppfølging er forhold rundt**
  - *Økt bruk av velferdsteknologi.*
  - *Behov for vurdering av sertifisering, selvdeklarering og attestasjon av leverandører, løsninger eller MTU.*
  - *Avklare omfang av særnorske krav rundt behandling av pasientinformasjon.*
  - *Veiledningsmateriale rundt sikkerhetsloven § 29 a, som omhandler varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til kritisk infrastruktur.*

I Nasjonal e-helsestrategi 2017–2022 er det et grunnleggende prinsipp at det som kan bli løst nasjonalt, skal bli løst nasjonalt. Å legge til rette for nye samhandlingsformer er viktige tiltak i strategiperioden. Dette omfatter blant annet:

- Tilgang mellom virksomheter
- Grunndataløft
- Økt sporbarhet
- Bedre pasientmedvirkning og informasjonsflyt
- Digital sikkerhetsstrategi for helsesektoren

Oppgavene må løses i fellesskap i sektoren. For å få dette til, er det viktig å etablere finansieringsmodeller som gjør det mulig. Direktoratet har anbefalt obligatorisk samfinansiering av viktige nasjonale løsninger.

2 Bakgrunn og formål

Helse- og omsorgsdepartementet (HOD) har gitt Direktoratet for e-helse følgende oppdrag:

1. *Direktoratet for e-helse gis i oppdrag å identifisere og foreslå gode rutiner for å sikre at de til enhver tid gjeldende krav til informasjonssikkerhet ved bruk av private leverandører etterleves.*

2. *Direktoratet skal som del av oppdraget utarbeide en overordnet status for bruk av nasjonale og internasjonale leverandører av tjenester som kontinuerlig eller episodisk arbeider inn mot virksomhetens datasystemer og under hvilke betingelser dette skjer.*

3. *Det skal videre utarbeides et sett med kriterier eller betingelser som bidrar til at denne formen for tjenester skjer på en ansvarlig måte og i tråd med de til enhver tid gjeldende krav.*

4. *Det er i denne sammenheng også relevant å vurdere om det er tjenester som ikke bør overlates til private leverandører. Spesielt har departementet sett behov for at det sees på hvilke situasjoner og hvordan det eventuelt bør og kan skilles mellom norske, EØS baserte og globale leverandører, herunder behovet for å se på forholdet mellom helsetjenesten og sikkerhetsloven.*

Som juridisk ramme for arbeidet vises det blant annet til helseforetaksloven §28, pasientjournalloven §22 og 23, personopplysningsforskriften kapittel 2, og forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten.

For å sikre et godt grunnlag skal Direktoratet for e-helse i sitt arbeid med oppdraget:

- *Invitere representanter fra spesialisthelsetjenesten, andre relevante helsetjenesteaktører og helseforvaltningsorganer som behandler pasient-informasjon til å delta i arbeidet.*
- *Invitere følgende aktørgrupper til å gi innspill:*
  - Andre sentrale kompetansemiljøer, herunder Nasjonal sikkerhetsmyndighet
  - Fagorganisasjoner, tillitsvalgte og brukerorganisasjoner
  - Representanter for IKT-næringen

Omfang og avgrensning

Oppdraget dekker informasjonssikkerhet knyttet til systemer som inneholder pasientinformasjon[1] og avgrenses til problemstillinger i forbindelse med sikkerhet ved bruk av private leverandører. Dette dekker tjenesteområdene basisdrift, applikasjonsdrift, applikasjonsforvaltning og applikasjonsutvikling (inkludert innføring) hvor man får tilgang til pasientinformasjon. Videre dekker oppdraget både mer omfattende tjenesteutsetting og mindre/tidsavgrensede tjenesteavtaler, inkluderer problemstillinger rundt medisinsk-teknisk utstyr. Oppdraget dekker ikke generell sikkerhet som intern tilgangsstyring, men sikkerhetsvurderinger som følger av endret risikobilde ved bruk av private leverandører omfattes.

Rapporten benytter stort sett begrepet «private leverandører». Dette inkluderer alle eksterne, nasjonale og internasjonale, leverandører. I noen tilfeller blir begrepet «globale leverandører» benyttet, da refereres det spesifikt til leverandører utenfor EU/EØS-området.

2.1 Aktørene og prosessen underveis

I oppdraget ble Direktoratet for e-helse bedt om å invitere representanter fra spesialisthelsetjenesten, andre relevante helsetjenesteaktører og helseforvaltningsorganer som behandler pasientinformasjon til å delta i arbeidet. I arbeidet har disse representantene blitt delt inn i fire hovedgrupper[2]:

- **Hovedaktørene** inkluderer de fire regionale helseforetakene[3], Helse Sør-Øst RHF (Helse Sør-Øst), Helse Vest RHF (Helse Vest), Helse Midt-Norge RHF (Helse Midt), Helse Nord RHF (Helse Nord) og andre helsetjenesteaktører som behandler pasientinformasjon, samt Sykehusinnkjøp og Nasjonal IKT.
- **Kompetansemiljøene** som består av Center for Cyber and Information Security (CCIS), Datatilsynet, Direktoratet for forvaltning og IKT (DIFI), Direktoratet for samfunnssikkerhet og beredskap (DSB), Nasjonal kommunikasjonsmyndighet (NKOM) og Nasjonal sikkerhetsmyndighet (NSM).
- **IKT-næringen**, bransjeforeninger og deres medlemmer.
- **Fag- og pasientorganisasjoner**.

Det er avholdt dialogseminarer med ovennevnte grupper og underveis i arbeidet har aktørene fått mulighet til å komme med informasjon og innspill.

I tillegg er det gjennomført særmøter med Nasjonal sikkerhetsmyndighet, Fagutvalget (NUFA), Datatilsynet, Helse Sør-Øst, Helseplattformen (Helse Midt), representant for fastlegene i EPJ-løftet, Pasient- og brukerombudet i Sogn og

1 Ordinære og sensitive personopplysninger.

2 En detaljert oversikt over hvilke aktører som deltok ligger i vedlegg 2.

3 Direktoratet for e-helse ba RHFene koordinere deltakelse fra sine underliggende enheter.

Fjordane og Oslo samt Apotekforeningen. Det er også mottatt informasjon om prosesser og erfaringer fra Telenor, Statoil og Finanstilsynet.

Kommuner

I utgangspunktet skulle kommunesektoren inkluderes i dette arbeidet. Det er sendt ut spørreskjemaer til et utvalg av kommuner, men det har ikke kommet inn tilstrekkelig antall svar for å danne et godt nok grunnlag for å besvare oppdraget fra HOD. Rapporten omhandler derfor ikke kommunesektoren. Kommunesektoren må eventuelt gjennomgås i en videreføring av prosessen.

Informasjonsinnhenting

Samtlige aktører som er involvert i arbeidet har fått mulighet til å komme med innspill ved å svare på tilsendt spørsmålskjema[4]. De øvrige aktørene har fått mulighet til å komme med innspill til oppdragets delleveranser, tilpasset deres posisjon[5].

Arbeidet med informasjonsinnhentingen avdekker at det er utfordrende å få en god oversikt over bruken av private leverandører i helse- og omsorgssektoren.

2.2 IKT-tjenesteområder dekket i rapporten

Det er flere ulike områder av IKT-tjenester som kan settes ut til private leverandører. I hovedsak faller disse inn i fire ulike tjenesteområder:

- Basisdrift
- Applikasjonsdrift
- Applikasjonsforvaltning
- Applikasjonsutvikling (inkludert innføring)

Under informasjonsinnhentingen og i denne rapporten benyttes disse begrepene. I noen kapitler kommenteres enkelte tjenesteområder samlet. For en utfyllende oversikt over begreper som er benyttet i denne rapporten, se vedlegg 1.

I dialogen med aktørene kommenterer noen bare på basisdrift. For å få oversikt over bruk av private leverandører er det viktig at alle tjenesteområdene inkluderes. Det er ulik risiko knyttet til private leverandørers tilgang til pasientinformasjon innenfor disse områdene, men alle kan medføre tilgang til pasientinformasjon. Det er også ulik måte å sikre tilgang til informasjon innenfor disse tjenesteområdene. Private leverandører kan enten ta ansvar for et tjenesteområde eller bidra på ulike deler av et tjenesteområde. Dette påvirker om og i hvilken grad private leverandører har tilgang til pasientinformasjon.

Det er en trend at grensen mellom disse tjenesteområdene viskes ut.

4 Spørreskjema i sin helhet ligger i vedlegg 4.

5 For en fullstendig oversikt over hvilke aktører som har gitt innspill og hvilke spørsmål de ulike aktørene fikk, se vedlegg 3.

Tjenesteområdene sammenstilles i leveranser primært gjennom tilgang til løsningene via skyløsninger.

Nedenfor er det en kort beskrivelse av de enkelte områdene og vurdering av risiko for at de som arbeider innenfor disse kan få tilgang til pasientinformasjon.

2.2.1 Basisdrift

Basisdrift er drift av underliggende infrastruktur og plattform som brukes til å levere applikasjoner til brukerne. Drift dreier seg om å sikre at disse leveres til avtalt nivå. Dette omfatter prosesser for håndtering av blant annet varsler, hendelser, henvendelser, problemer og tilganger. Det omfatter også funksjoner som ulike former for teknisk styring. Basisdrift medfører at driftspersonell får tilgang til komponenter som kan inneholde pasientopplysninger og styring av hvem som har tilgang. De som administrerer infrastruktur kan for eksempel slette logger for å fjerne spor etter egen aktivitet, og eventuelt endre eller ødelegge data.

Infrastruktur og plattform dekker komponenter som maskinvare, nettverk, operativsystem og databaser. Dette dekker også basis programvare for å understøtte integrasjoner, identitet- og tilgangsstyring

2.2.2 Applikasjonsdrift

Applikasjonsdrift er også drift, men av applikasjoner. En applikasjon er bruker-rettet programvare. På et sykehus er pasientadministrativt system (PAS), elektronisk journal, kurve, radiologi- og bildesystem og laboratoriesystem noen av de viktigste applikasjonene. Personell som driver med applikasjonsdrift vil ofte ha tjenstlig behov for tilgang til produksjonsdata. For kliniske systemer betyr dette tilgang til pasientinformasjon.

2.2.3 Applikasjonsforvaltning

Applikasjonsforvaltning er funksjonen som administrerer applikasjoner gjennom deres livssyklus. Dette dreier seg for eksempel om vedlikehold i form av feil-rettinger og endringer i oppsett for å håndtere endrede behov, samt planlegging, testing og gjennomføring av oppdateringer og mindre oppgraderinger.

Applikasjonsforvaltning medfører ikke nødvendigvis at man har tilgang til produksjonsdata. Skillet mellom forvaltning og drift kan legges slik at forvaltning ikke har tilgang til produksjonssystemer. Likevel har gjerne personell som arbeider med applikasjonsforvaltning tilgang til pasientinformasjon. Dette skyldes blant annet at det kan være vanskelig å gjenskape feil i et annet miljø uten produksjons-data og det kan være vanskelig å utarbeide testdata som er dekkende nok uten å bruke reelle data. For å løse akutte feilsituasjoner må de som forvalter løsningen, i noen tilfeller, også gis tilgang direkte til produksjonssystemer med pasientinformasjon.

2.2.4 Applikasjonsutvikling og -innføring

Applikasjonsutvikling og -innføring dekker utvikling av programvare, sette opp og integrere nye systemer, eller gjøre omfattende endringer i eksisterende programvare utover vanlig vedlikehold som gjøres som en del av forvaltningen.

I likhet med applikasjonsforvaltning medfører ikke denne type tjenester nødvendigvis behov for tilgang til produksjonsdata. Likevel kan det være tilfeller der slik tilgang gjør det enklere eller nødvendig. Dette gjelder spesielt utvikling av integrasjoner, rapporter og programmer for konvertering av data der reelle data gjør det enklere for utvikleren å forstå datastrukturer og innhold. I tillegg kan det også her være vanskelig å utarbeide testdata som er dekkende nok uten å bruke reelle data.

3 Juridiske vurderinger og teknologiske trender

3.1 Juridiske vurderinger

3.1.1 Oppsummering av hovedpunktene

Ansvar for informasjonssikkerhet og behandling av person-opplysninger

Det er den databehandlingsansvarlige som må sørge for å ivareta forsvarlig informasjonssikkerhet og tilfredsstille det til enhver tid gjeldende regelverk for behandling av personopplysninger. Databehandlingsansvaret ligger hos ledelsen av virksomheten.

Om bruk av private leverandører

I gjeldene rett er det ikke noe forbud mot at norske virksomheter benytter nasjonale eller utenlandske, private leverandører fra EU/EØS-området. Ved bruk av globale leverandører (utenfor EU/EØS) er det særskilte krav som må oppfylles.

Anskaffelsesrettslige forhold

Anskaffelsesregelverket legger ikke noen generelle begrensninger på hvor produkter og tjenester kan anskaffes fra. Anskaffelser skal som hovedregel kunngjøres til hele det indre marked (EU/EØS). Anskaffelsesregelverket er heller ikke til hinder for bruk av leverandører utenfor EU/EØS.

Forhold mellom sikkerhetsloven og helsetjenesten.

Forholdet mellom sikkerhetsloven og helsetjenesten er et område i bevegelse. Det er nylig innført endringer i sikkerhetsloven og forslag til ny sikkerhetslov er fremmet for Stortinget. Det er en usikkerhet blant flere aktører i sektoren om sikkerhetsloven får anvendelse på deres aktivitet og behov for veiledning om dette.

Ny personopplysningslov og EUs personvernforordning (GDPR)

Forordningen bidrar til harmonisering av personvernreglene i EU/EØS og vil gjelde som lov i Norge. Det er ett av formålene med forordningen å skape et felles regelverk for personvern i hele det indre marked. Det bidrar til å styrke europeiske borgeres rettigheter og gjør det samtidig enklere for leverandører å tilby sine løsninger i flere land. Forordningen medfører flere rettigheter for den registrerte (personen opplysningene omhandler) og flere forpliktelser for de som behandler personopplysninger.

3.1.2 Ansvar for informasjonssikkerhet og behandling av personopplysninger

Rettslig regulering av informasjonssikkerhet og behandling av personopplysninger i helse- og omsorgssektoren følger av:

1. *Generell regulering* i lov og forskrift om behandling av personopplysninger.
2. *Sektorspesifikk lovgivning*, særlig pasientjournalloven og helseregisterloven med forskrifter.
3. «Norm for informasjonssikkerhet i helse- og omsorgstjenesten». Normen er en bransjenorm utarbeidet i fellesskap av sektoren. Normen er bindene gjennom avtale da Norsk Helsenett (NHN) forutsetter at tilknyttede parter forplikter seg til å følge Normen.

Det er den databehandlingsansvarlige som må sørge for å ivareta forsvarlig informasjonssikkerhet og tilfredsstille det til enhver tid gjeldende regelverk for behandling av personopplysninger. Pasientjournalloven definerer begrepet databehandlingsansvarlig i § 2 e: *«Databehandlingsansvarlig: den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, og den som i eller i medhold av lov er pålagt et databehandlingsansvar.»*

Den databehandlingsansvarlige kan benytte andre, herunder private leverandører, til å behandle personopplysninger på sine vegne. Bruk av databehandler[6] er regulert i personopplysningsloven § 15: *«En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse. I avtalen med den behandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13.»*

En databehandlingsansvarlig vil typisk være et helseforetak, et legekontor eller annen virksomhet som samler inn eller behandler personopplysninger. En privat leverandør som for eksempel på vegne av helseforetaket behandler opplysninger, vil typisk være en databehandler.

Internkontroll

Etter pasientjournalloven § 23 om internkontroll har den databehandlingsansvarlige plikt til å etablere og holde ved like planlagte og systematisk tiltak som er nødvendige for å oppfylle kravene i eller i medhold av loven. Tiltakene skal dokumenteres.

6 Personopplysningsloven § 2 nr. 5. Databehandler: den som behandler personopplysninger på vegne av den databehandlingsansvarlige.

Informasjonssikkerhet

Pasientjournalloven § 22 omhandler sikring av konfidensialitet, integritet og tilgjengelighet av helseopplysninger. Kravene kan oppsummeres på følgende måte:

- Den databehandlingsansvarlige og databehandleren skal sørge for tilfredsstillende informasjonssikkerhet gjennom planlagte og systematiske tiltak. Dette omfatter blant annet å sørge for tilgangsstyring, logging og etterfølgende kontroll.
- Det påhviler den databehandlingsvarlige og databehandleren å dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeidere hos begge parter og for tilsynsmyndigheter.
- En databehandlingsansvarlig som lar andre få tilgang til helseopplysninger, for eksempel en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at også disse oppfyller kravene i paragrafen.
- Dette pålegger og understreker at det er den databehandlingsansvarlige som har ansvar for at også databehandlere og andre oppfyller kravene til informasjonssikkerhet. Dette ansvaret kan ikke overføres til andre.

Personopplysningsforskriftens kapittel 2

Personopplysningsforskriftens kapittel 2 handler om informasjonssikkerhet. Alle bestemmelsene i kapittelet er i utgangspunktet relevante ved vurdering av informasjonssikkerhet, også ved bruk av private leverandører. Her nevnes noen bestemmelser som er spesielt aktuelle for problemstillingen gitt i oppdraget:

- Forskriftens § 2-3 sier uttrykkelig at den daglige ledelsen av virksomheten som den behandlingsansvarlige driver, har ansvar for at bestemmelsene om informasjonssikkerhet følges.
- Forskriftens § 2-4 om risikovurdering pålegger virksomheten å føre en oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptable risiko forbundet med behandlingen. Den databehandlingsansvarlige skal videre gjennomføre risikovurderingen. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.
- Forskriftens § 2-5 omhandler pålegg og regulering av ansvar for sikkerhetsrevisjon, herunder sikkerhet hos leverandører.
- Forskriftens § 2-15 omhandler sikkerhet hos andre virksomheter. Blant annet er det regulert at leverandører har et selvstendig ansvar for å ivareta informasjonssikkerhet. Videre pålegges den databehandlingsansvarlige både å etablere klare ansvars- og myndighetsforhold, ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, samt jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.[7]

7 Normen punkt 5.8.1 og 5.8.2.

Helseforetaksloven

Lovens formål (se § 1) er å bidra til å oppfylle målsetninger i spesialisthelse-tjenesteloven og pasient- og brukerrettighetsloven ved at det opprettes regionale helseforetak som skal planlegge og organisere spesialist-helsetjenesten. Det legges til rette for at de regionale helseforetakene skal organisere sine sykehus som helseforetak. Helseforetakenes formål er å yte gode og likeverdige spesialisthelsetjenester til alle som trenger det når de trenger det.

Regionalt helseforetak eies av staten alene (se § 2) og har et overordnet ansvar for å iverksette den nasjonale helsepolitikken i helseregionen (se § 2a). Regionale helseforetak skal planlegge, organisere, styre og samordne virksomhetene i helseforetakene de eier. Utøvende virksomhet skal organiseres som helseforetak (se § 9). Både regionale helseforetak og helseforetak ledes av et styre og en daglig leder (se § 20).

Daglig leder forestår den daglige ledelsen av foretaket (se § 37). Det innebærer at vedkommende har ansvaret for informasjonssikkerheten knyttet til behandling av personopplysninger i foretaket, se omtale av personopplysningsforskriften ovenfor.

Etter § 28 hører forvaltningen av foretaket under styret. Styret har ansvar for en tilfredsstillende organisering av foretakets samlede virksomhet. Styret skal holde seg orientert om foretakets virksomhet og økonomiske stilling, og føre tilsyn med at virksomheten drives i samsvar med målene i lovens § 1 (formålet), foretakets vedtekter, vedtak truffet av foretaksmøtet og vedtatte planer og budsjetter. I regionalt helseforetak omfatter styrets plikter også de helseforetak som det regionale helseforetaket eier.

Den daglige ledelsen omfatter ikke saker som etter foretakets forhold er av uvanlig art eller av stor betydning (se § 37). I slike tilfeller skal styret underrettes og kan eventuelt gi daglig leder myndighet til å avgjøre saken. Daglig leder kan også treffe avgjørelse dersom styrets beslutning ikke kan avventes uten vesentlig ulempe for foretakets virksomhet. Det kan tenkes forhold knyttet til informasjonssikkerhet som har en slik alvorlig karakter, for eksempel vesentlige sikkerhetsbrudd hvor pasientopplysninger kommer på avveie.

Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten

Forskriften har som formål å bidra til faglig forsvarlig helse- og omsorgtjenester, kvalitetsforbedring og pasient- og brukersikkerhets og at øvrige krav i helse- og omsorgslovgivningen etterleves.

Forskriften pålegger virksomheter[8] plikt til å planlegge, gjennomføre, evaluere og korrigere virksomhetens aktiviteter, samt at dette skal dokumenteres og

8 Se forskriftens § 2 for hvilke virksomheter som er omfattet.

styres gjennom et styringssystem[9]. Kravene til internkontroll og informasjonssikkerhet i regelverket om behandling av personopplysninger, bør innarbeides i det samme styringssystemet og følges opp av ledelsen som en del av virksomhetens samlede styringssystem.

3.1.3 Om bruk av private leverandører – personvernperspektiv

Nasjonale og EU/EØS-baserte leverandører

Bruk av private leverandører er utbredt og en nødvendighet for sektoren. Det er ikke noe generelt forbud imot å benytte nasjonale eller EU/EØS-baserte leverandører i gjeldende lovgivning. Etter personopplysningsloven § 29 kan personopplysninger overføres til stater som sikrer en forsvarlig behandling av opplysningene. Landene innenfor EU/EØS har innført EUs personverndirektiv 95/46/EF og oppfyller dette kravet. En målsetning med direktivet var at medlemslandene ikke skal hindre eller forby fri flyt av personopplysninger mellom landene av hensyn til personvernet.

Spesiallovgivningen for helse- og omsorgssektoren, særlig relevant her pasientjournalloven, har ingen direkte regulering om overføring eller annen behandling av helseopplysninger mot utlandet. Personopplysningsloven kommer da til anvendelse, dette følger av pasientjournalloven § 5.

Gjeldene arkivlov har et forbud mot at arkivopplysninger lagres i utlandet, jf. arkivloven § 9 bokstav b. Dette er et forbud som er foreslått fjernet i høring[10] om ny forskrift om offentlige arkiv.

Oppsummering

Det er i gjeldene rett ikke noe forbud mot at norske virksomheter benytter nasjonale eller utenlandske, private leverandører fra EU/EØS-området som databehandlere.

Globale leverandører

Dersom helseopplysninger skal overføres til såkalte tredjeland, det vil si land utenfor EU/EØS, gjelder noen særskilte krav i tillegg til de øvrige kravene i personopplysningsloven. Dette er regulert i personopplysningsloven § 29 og § 30.[11]

Begrepet overføring, som er lovens ordlyd, er ikke begrenset til faktisk overføring (fysisk overføring eller «flytting»), men omfatter også tilfeller der noen har tilgang fra utlandet, for eksempel via fjernaksess. Dette er en relevant

9 Se forskriftens § 4 for definisjon av styringssystem.

10 Se https://www.regjeringen.no/no/dokumenter/hoyring--ny-forskrift-om-offentlege-arkiv/id2515364/

11 Se også Datatilsynets hjemmesider for en mer fullstendig oppsummering og veiledning: https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/overfore/

og økende form for behandling av personopplysninger, ettersom for eksempel teknisk drift og fjernsupport følger nye leveransemodeller som skybaserte tjenester og support fra hele verden.

Utgangspunktet etter § 29 er at personopplysninger bare kan overføres til stater som sikrer forsvarlig behandling av opplysningene. For land utenfor EU/EØS må det foretas en konkret vurdering av om behandlingen sikres på forsvarlig måte. Opplysninger kan også overføres til land Europakommisjonen har godkjent.[12] Et hovedpoeng er at databehandlingsansvarlig må forsikre seg om at personopplysningslovens øvrige vilkår er oppfylt samt oppnå tilstrekkelige garantier for vern av den registrertes rettigheter. For eksempel er egne avtaler og fremgangsmåter utarbeidet for overføring og bruk av underleverandører i enkelte jurisdiksjoner. Et eksempel er «Privacy Shield» som kan benyttes ved overføring av opplysninger til USA (som et av flere lovlige alternativer). «Privacy Shield» er et juridisk rammeverk som er utarbeidet for å beskytte europeiske personvernrettigheter når opplysninger overføres fra Europa til USA. Rammeverket erstatter den tidligere mekanismen «Safe Harbor» og er ment å muliggjøre og forenkle transatlantisk elektronisk overføring av opplysninger og samarbeid.

Oppsummering

Det er i gjeldene rett ikke forbud mot at norske virksomheter benytter globale private leverandører utenfor EU/EØS-området som databehandlere, forutsatt at leverandørene sikrer en forsvarlig behandling av personopplysninger.

3.1.4 Anskaffelsesrettslige forhold

De fleste aktørene i helse- og omsorgssektoren er underlagt lov om offentlige anskaffelser. Loven gjennomfører EØS-direktivene om offentlige anskaffelser og gir rammer og krav til hvordan anskaffelser skal gjennomføres.

Oppdragsgiver skal ved anskaffelser opptre i samsvar med de grunnleggende prinsippene om konkurranse, likebehandling, forutberegnelighet, etterprøvbarhet og forholdsmessighet. Dette omfatter også at det ikke skal utøves ulovlig diskriminering av aktørene i det europeiske markedet. Dette er bakgrunnen for at anskaffelser over fastsatte terskelverdier må kunngjøres i EU/EØS.

Forbudet mot diskriminering på bakgrunn av nasjonalitet innebærer at oppdragsgiver ikke kan stenge leverandører ute fra konkurransen basert på antagelser som kan bli rammet av ikke-diskrimineringsforbudet.

Oppdragsgiver må spesifisere krav til leveransen for å møte de behov som anskaffelsen er ment å dekke. Anskaffelse av IKT-løsninger og tjenester i sektoren vil normalt omfatte behandling av personopplysninger og krever god kjennskap til personopplysnings-regelverket og spesiallovgivningen. Det må

12 Se http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

stilles krav for å ivareta personvernet og tilfredsstillende informasjonssikkerhet. I tillegg vil det være mulig å for eksempel stille krav om at tilbyder ikke skal behandle opplysninger i eller fra bestemte jurisdiksjoner som ikke sikrer forsvarlig behandling av personopplysningene.

I henhold til anskaffelsesregelverket er det i utgangspunktet liten mulighet til å skille mellom norske leverenadører og leverandører fra EU/EØS-området. Unntaket er anskaffelser som gjelder sikkerhetsmessige forhold, jf. anskaffelsesforskriften § 2-2. Dette gjelder for eksempel der sikkerhetsloven kommer til anvendelse.

Oppsummering

Anskaffelsesregelverket har ikke noen generelle begrensninger på hvor produkter og tjenester kan anskaffes fra. Anskaffelser skal som hovedregel kunngjøres til hele det indre marked (EU/EØS). Anskaffelsesregelverket er heller ikke til hinder for bruk av leverandører utenfor EU/EØS.

3.1.5 Forhold mellom helsetjenesten og sikkerhetsloven

Sikkerhetsloven har til formål å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, ivareta den enkeltes rettssikkerhet og trygge tillitten til den forebyggende sikkerhetstjeneste, se lovens § 1.

Flere aktører i sektoren har tidligere vurdert om sikkerhetslovens bestemmelser om skjermingsverdig objekt eller informasjon, kommer til anvendelse innen IKT-området. De vurderingene vi har fått kjennskap til, har konkludert med at sikkerhetslovens regler om skjermingsverdige objekter[13] til nå ikke har kommet til anvendelse.

1. januar 2017 trådte et nytt kapittel 7 «*Sikkerhetsgraderte anskaffelser og anskaffelser til kritisk infrastruktur*» i kraft. I tillegg ligger forslag til ny sikkerhetslov til behandling i Stortinget. Utkastet til ny sikkerhetslov er en modernisering tilpasset den teknologiske utviklingen. Ifølge Forsvarsdepartementet vil den nye loven favne bredere og være mer dynamisk og fleksibel. I pressemeldingen[14] fra lovforslaget som ble fremmet 16.06.2017 heter det:

«Den teknologiske utviklingen har gjort det nødvendig å revidere og modernisere loven. Loven vil styrke samhandlingen mellom myndigheter og virksomheter slik at det forebyggende sikkerhetsarbeidet mot terror, sabotasje og spionasje kan gjennomføres på en mer effektiv og forsvarlig måte på tvers av samfunnssektorene.»

13 jf. lovens § 17

14 https://www.regjeringen.no/no/aktuelt/modernisert-sikkerhetslov-som-favner-bredere/id2557584/

Det skal utarbeides forskrifter til den nye loven og det nye regelverket vil trolig tre i kraft tidligst 1.1.2019. Fra dialog med aktører i sektoren, synes det å være usikkerhet rundt både hvilke deler av sikkerhetsloven som er relevant og hvilke konsekvenser dette har. Kort oppsummert, er det usikkerhet om:

- Hva som faller inn under utrykket «*kritisk infrastruktur*» i sikkerhetsloven.
- Usikkerhet eller sammenblanding av hvilke plikter/konsekvenser de nye bestemmelsene om «kritisk infrastruktur» har versus plikter/konsekvenser etter lovens kapittel 5 om objektsikring.
- Bekymringer om nylige endringer, ny sikkerhetslov eller sikkerhetslovens kapittel 5 vil komme til anvendelse, og om det innebærer at personell må ha sikkerhetsklarering eller autorisasjon etter sikkerhetsloven. Dette anses som spesielt utfordrende å implementere i forbindelse med pasientjournal-systemene og andre systemer med mange brukere.

Om sikkerhetsloven § 29 a

Bestemmelsen omhandler varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til kritisk infrastruktur. Bestemmelsen medfører ikke krav til sikkerhetsklarering.

Utrykket «*kritisk infrastruktur*» er definert i § 3 nr. 21 som: «*anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner*.»

Forarbeidene[15] gir noen kriterier for å vurdere hvorvidt et system eller anlegg skal regnes som «*kritisk infrastruktur*». For å besvare dette, må man etter forarbeidene vurdere 1) hva som er samfunnets grunnleggende behov, 2) hvilke samfunnsfunksjoner som er kritiske for å dekke disse behovene og 3) hva slags systemer og anlegg som er helt nødvendige for å opprettholde disse funksjonene[16].

Direktoratet for e-helse har hatt dialog med Nasjonal sikkerhetsmyndighet. De uttaler at hvorvidt et IKT-system er en del av kritisk infrastruktur må avklares med overordnet departement.

Når det foretas anskaffelser til noe som kan bli vurdert som «kritisk infra-struktur», pålegger § 29 a:

(1) At det foretas en risikovurdering. I vurderingen skal det tas stilling til om anskaffelsen innebærer en ikke ubetydelig risiko for at «*sikkerhetstruende virksomhet*» blir etablert eller gjennomført. «*Sikkerhetstruende virksomhet*» er definert i § 3 nr. 2 som «*forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet*». Dersom en i vurderingen finner risiko for at «*sikkerhetstruende virksomhet*» blir

15 Prop. 97 L (2015-2016), se særlig punkt 13 og som viser videre til punkt 11.1.2 og 11.4.7.

16 Prop. 97 L (2015-2016) på side 51.

etablert, og man ikke klarer å iverksette tiltak som fjerner eller gjør risikoen ubetydelig, utløser dette en

(2) Varslingsplikt til overordnet departement. Departementet bør deretter innhente rådgivende uttalelse fra relevante organer om leveransens risikopotensial, og leverandørens sikkerhetsmessige pålitelighet.

Dersom en anskaffelse til kritisk infrastruktur kan medføre en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert, kan Kongen i statsråd

(3) Fatte vedtak om at anskaffelsen stanses eller gi vilkår for gjennomføring. Dersom det ikke fattes slikt vedtak, skal departementet underrette virksomheten. Kongen i statsråd kan også gi forskrift om anskaffelser til kritisk infrastruktur. Slik forskrift er ikke gitt.

I forarbeidene[17] fremgår det at: «*Kongen i statsråd kan tillate anskaffelsen, tillate anskaffelsen på visse vilkår, eller nekte anskaffelsen gjennomført. Avgjørelsen vil måtte baseres på en helhetsvurdering der sikkerhetshensyn står sentralt, men der det også tas hensyn til blant annet økonomiske forhold og ønsket om hensiktsmessig utvikling av infrastruktur og næringsvirksomhet*.»

Oppsummering

Forholdet mellom sikkerhetsloven og helsetjenesten er et område i bevegelse. Det er nylig innført endringer i sikkerhetsloven og forslag til ny sikkerhetslov er fremmet for Stortinget. Det er en usikkerhet blant flere aktører i sektoren om sikkerhetsloven får anvendelse på deres aktivitet og det er behov for veiledning om dette.

3.1.6 Ny personopplysningslov og EUs personvernforordning (GDPR)

EUs personvernforordning, General Data Protection Regulation (GDPR), trer i kraft 25. mai 2018 og avløser personverndirektivet av 1995. Forordningen er EØS-relevant. En forordning er en EU-lov som gjelder etter sin ordlyd direkte i EUs medlemsstater. Når forordningen er innlemmet i EØS-avtalen vil den også gjelde i Norge.

Forordningen er foreslått implementert i Norge gjennom en ny personopplysningslov. Lovutkastet har nylig vært på høring. Den nye loven og forordningen vil erstatte nåværende personopplysningslov og tilhørende forskrifter. Den nye personopplysningsloven inneholder generelle bestemmelser om behandling av personopplysninger, der forordningen pålegger eller åpner for nasjonale regler. Sektorspesifikke regler skal fortsatt gis i særlovgivningen. Helse- og omsorgsdepartementet arbeider med tilpasninger i helselovgivningen som følge av forordningen.

17 Prop. 97 L (2015-2016) på side 55.

Forordningen består av 99 artikler og 173 fortalepunkter, og inneholder både oppdaterte og nye regler. Grunnprinsippene som ble nedfelt i EUs personvern-direktiv videreføres og det er tatt inn bestemmelser som klargjør flere rettigheter som er etablert gjennom europeisk rettspraksis. Mange av kravene til behandling av personopplysninger videreføres fra dagens regelverk og det innføres en del nye regler som alle som behandler personopplysninger må ta hensyn til. Blant de viktigste nye kravene er:

1. Styrking av den registrertes rettigheter

Den registrerte får noen nye rettigheter, for eksempel retten til dataportabilitet (det vil si retten til å ta med seg sine elektroniske personopplysninger fra en virksomhet til en annen). Det stilles også mer detaljerte krav til hvordan virksomhetene skal oppfylle den registrertes rettigheter.

2. Flere plikter for databehandlingsansvarlig og databehandler

Databehandlingsansvarlig og databehandler har både selvstendige og felles plikter. Nye plikter for databehandlingsansvarlig og databehandler kan oppsummeres slik:

- Skjerpede krav til innhold i databehandleravtaler[18]. Dette er avtaler som nærmere regulerer hvordan databehandler skal behandle person-opplysninger på vegne av databehandlingsansvarlig.
- Både databehandlingsansvarlig og databehandler skal ha oversikt over alle behandlinger av personopplysninger.
- Databehandlingsvarlig og databehandler må i visse tilfeller også oppnevne et eget personvernombud[19].

3. Strengere krav til samtykke

Samtykkeskjema må være klart, konsist og ikke unødvendig forstyrrende for bruken av tjenesten. Inaktivitet/passivitet er ikke lovlig samtykke.

4. Krav til innebygd personvern og personvern som standardinnstilling

Virksomheter som behandler personopplysninger må bygge personvern inn i løsningene[20]. Det skal tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Det minst personverninngripende alternativet skal brukes.

5. Krav til vurdering av personvernkonsekvenser

Virksomheter som skal behandle personopplysninger som sannsynligvis vil utgjøre høy risiko for personers rettigheter, må utrede personvern-konsekvensene før behandlingen tar til.

6. Strengere krav til avvikshåndtering

Alle avvik som skyldes brudd på personopplysningssikkerheten skal meldes til

18 For oppsummering av krav til innhold i databehandleravtaler, se https://www.datatilsynet.no/regelverk-og-skjema/veiledere/hva-betyr/?id=6326

19 For en oppsummering, se https://www.datatilsynet.no/regelverk-og-skjema/veiledere/hva-betyr/?id=6324

20 Se https://www.datatilsynet.no/regelverk-og-skjema/lage-nye-losninger/innebygd-personvern/

Datatilsynet. Det stilles krav til at avviksmeldingen skal leveres til Datatilsynet innen 72 timer. Dersom virksomheten ikke har full oversikt over avviket, kan de sende avviksmeldingen trinnvis.

7. Strengere sanksjoner
Datatilsynet får mulighet til å ilegge vesentlig høyere overtredelsesgebyr (opp til EUR 20 millioner eller 4 prosent av global omsetning).

Spesielt for den databehandlingsansvarlige

Databehandlingsansvarlig får utvidet plikt til å vurdere personvernkonsekvenser ved behandling av personopplysninger. Databehandlingsansvarlig får også plikt til å identifisere risikoreduserende tiltak. Der risikoen ikke kan håndteres på en tilfredsstillende måte av virksomheten, skal virksomheten gjennomføre forhåndsdrøftinger med Datatilsynet.

Databehandlingsansvarlig skal etter GDPR godkjenne databehandleres eventuelle underleverandører.

Databehandlingsansvarlig har alltid hovedansvaret for behandling av personopplysninger, og kan aldri overføre ansvaret til andre selv om oppgaver som for eksempel drift er overført til en databehandler.

Spesielt for databehandler

Databehandlere vil etter GDPR få plikt til å bistå databehandlingsansvarlig med etterlevelse av forordningen. Databehandler må dokumentere behandling av personopplysninger som foretas for hver enkelt databehandlingsansvarlig. Databehandler skal kun behandle personopplysninger basert på avtale med databehandlingsansvarlig.

Databehandlere må søke om forhåndsgodkjenning fra databehandlingsansvarlig ved bruk av eventuelle underleverandører.

Anledning til å begrense overføring av sensitive personopplysninger til tredjeland

Forordningens artikkel 49 nr. 5 åpner for at det i nasjonal rett, av hensyn til viktige samfunnsinteresser, kan fastsettes begrensninger for overføring av sensitive personopplysninger til en tredjestat eller en internasjonal organisasjon. Dette gjelder i tilfeller hvor det ikke foreligger en beslutning fra Kommisjonen om tilstrekkelig beskyttelsesnivå for tredjestat, et territorium eller en bestemt sektor i en tredjestat.

Justisdepartementets vurdering i høringsnotatet er at det ikke foreslås å lovfeste slike begrensninger nå. Departementet foreslår en lovhjemmel for senere å kunne forskriftsregulere slike begrensninger.

Oppsummering

Forordningen bidrar til harmonisering av personvernreglene i EU/EØS og vil gjelde som lov i Norge. Ett av formålene med forordningen er å skape et felles regelverk for personvern i hele det indre marked. Det bidrar til å styrke europeiske borgeres rettigheter og gjør det samtidig enklere for leverandører å tilby sine løsninger i flere land.

Forordningen medfører flere rettigheter for den registrerte og flere forpliktelser for de som behandler personopplysninger. Sektorspesifikke regler skal fortsatt gis i særlovgivningen. Det er også et formål med forordningen å styrke tillitten til digitale tjenester og dermed legge til rette for ytterligere digitalisering.

Strengere regler og høyere bøtenivå som følger av forordningen antas å øke oppmerksomheten på personvern både i anskaffelser, virksomhetsstrategier og ledelsesbeslutninger generelt.

3.1.7 Stortingsmeldinger, rapporter og andre relevante utredninger

Det er utarbeidet flere stortingsmeldinger, utredninger og rapporter vedrørende informasjonssikkerhet i helse- og omsorgsektoren. Nedenfor presenteres noen som Direktoratet for e-helse mener er relevante for problemstillinger i rapporten.

Meld. St. 9 (2012–2013) Én innbygger – én journal

I stortingsmeldingen beskrives følgende overordnede mål for IKT-utviklingen i helse- og omsorgstjenesten:

- Helsepersonell skal ha enkel og sikker tilgang til pasient- og brukeropplysninger.
- Innbyggerne skal ha tilgang på enkle og sikre digitale tjenester.
- Data skal være tilgjengelig for kvalitetsforbedring, helseovervåking, styring og forskning.

Med tanke på informasjonssikkerhet og personvern, kan sikker tilgang for helsepersonell og brukere bety at både konfidensialitet, integritet og tilgjengelighet skal sikres. Sett i lys av temaet for denne rapporten, må bruk av private leverandører skje på en slik måte at det understøtter målene om sikker tilgang til opplysninger og tjenester.

Meld. St. 38 (2016–2017) IKT-sikkerhet — Et felles ansvar

Meldingen presenterer regjeringens IKT-sikkerhetspolitikk. Det gis en oversikt over status på oppfølgingen av anbefalinger i NOU 2015: 13 Digital sårbarhet – sikkert samfunn. I tillegg vektlegges utvalgte områder som regjeringen mener er av særlig betydning for nasjonal IKT-sikkerhet.

Stortingsmeldingen omtaler tjenesteutsetting spesielt. Det uttales at tjenesteutsetting av IKT-tjenester til profesjonelle aktører vil kunne gi bedre sikkerhet og mer stabile og tilgjengelige tjenester, lavere og mer forutsigbare kostnader og bidra til bedre prioritering av virksomhetens kjerneområder. Samtidig understrekes det at virksomheten må ha god bestillerkompetanse og være bevisst hvilke verdier som eksponeres ved tjenesteutsetting, og iverksette nødvendige tiltak. Både behov for konfidensialitet, integritet, tilgjengelighet og regulatoriske krav bør inngå i vurderingene. Stortingsmeldingen inneholder en egen omtale av IKT-tjenesteutsetting i helsetjenesten. Her omtales Helse Sør-Øst sin plan for bruk av private leverandører i deres modernisering av IKT-infrastruktur (iMod), samtidig som det uttales at tjenesteutsetting til eksterne driftsoperatører fordrer kontrollregimer og risiko- og sårbarhetsanalyser som sikrer at krav til behandling av personopplysninger ivaretas.

NOU 2015:13 Digital sårbarhet – sikkert samfunn

Beskytte enkeltmennesker og samfunn i en digitalisert verden (Lysneutvalget I)

Utvalget kartlegger samfunnets digitale sårbarhet og foreslår tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Utredningen gjennomgår digitale sårbarheter innenfor flere samfunnsfunksjoner. For helse er det belyst at sektoren er svært sårbar for bortfall av elektronisk kommunikasjon (ekom).

Utvalget ser også på andelen av IKT-hendelser hos helseforetakene og Norsk Helsenett som er forårsaket av underleverandører, og finner at de står for en stor del av hendelsene på IKT-siden.

> «Tre av de regionale helseforetakene har rapportert til Lysneutvalget at henholdsvis 17–20 prosent, 26 prosent og 50 prosent av hendelsene skyldes svikt hos underleverandører. Ett av helseforetakene oppgir at de ikke har oversikt over dette. Norsk Helsenett anslår at omkring 80 prosent av større uønskede IKT-hendelser innenfor deres ansvarsområde er forårsaket av underleverandører. En stor andel av disse skyldes kommunikasjonsbrudd som har rammet større eller mindre grupper av kundene.»
>
> *NOU 2015:13 Digital sårbarhet – sikkert samfunn*

Det blir videre i utredningen tatt opp problemstillingen om at små og mellomstore private helseforetak ofte har begrensede ressurser til IKT-drift, og at mange har lagt for liten vekt på å utarbeide og implementere styringssystemer for informasjonssikkerhet.

Helsedirektoratets rapport «Overordnede risiko- og sårbarhets-vurderinger i helse- og omsorgssektoren» (06/2017)

I rapporten blir det trukket frem at pasientbehandling og pasientsikkerhet i økende grad blir avhengig av IKT og at digitale angrep kan forårsake at kritiske systemer blir utilgjengelige.

De viktigste sårbarhetene knyttet til IKT i sektoren blir definert til:

- Avhengighet til systemer og infrastruktur.
- Avhengigheter (ekom, strøm, vann).
- Utfordringer i elektronisk meldingsutveksling.
- Manglende høytilgjengelighet.
- Gammelt utstyr/programvare som ikke kan oppdateres.
- Et bredt spekter av angrepsvektorer mot sykehus og pasienter.
- Kommersielle interesser.
- Manglende oversikt, lange verdikjeder og gjensidig avhengighet.

Mens noen av rotårsakene som ligger til grunn for IKT sårbarhetene listet i rapporten ble indentifisert til:

- Manglende forståelse for IKT og informasjonssikkerhet som en del av det totale trusselbildet.
- Mangler eller svakheter i den enkelte virksomhets styringssystem for informasjonssikkerhet (ISMS).
- For få øvelser med «IKT» og «cyber» på agendaen.
- Manglende risikoanalyser.
- Manglende fokus på metode, systematikk og regelmessighet for gjennomføringer av ROS.
- Fragmentert myndighetsutøvelse.

Deler av konklusjonen fra rapporten er at IKT-området trenger økt oppmerksomhet og prioritering for å møte det stadig voksende trusselbildet som utvikler seg i takt med digitaliseringen. Rapporten trekker også frem at de lange og digitale verdikjedene, som spenner over sektorer, forvaltningsnivåer og land samt private og offentlige leverandører, bør være gjenstand for en mer helhetlig vurdering av gjensidige avhengigheter i beredskapssammenheng.

Helse Sør-Øst RHF Rapport fra ekstern gjennomgang av programmet for modernisering av IKT-infrastruktur (iMod) (juni 2017)

PwC har utført en utvidet revisjon av påstander om at eksterne tilganger til Helse Sør-Øst sin IKT-infrastruktur har gitt tilganger til sensitive person-opplysninger, herunder helseopplysninger.

PwCs hovedfunn og vurderinger er:

- Sykehuspartner HF har ikke tilstrekkelig kontroll på tilgangsstyring.
- Sykehuspartner HF har ikke tilstrekkelig sporbarhet på tilgang til helseopplysninger.
- 36 personer tilknyttet ESN-avtalen har hatt utvidede administratorrettigheter som innebærer mulighet for tilgang til helseopplysninger.
- Hewlett-Packard Norge AS/Enterprise Services Norge AS har så langt ikke kunnet dokumentere at det foreligger databehandleravtaler med samtlige underleverandører som oppfyller kravene i avtalen med Sykehuspartner HF.
- Systemet for gjennomføring av risikovurderinger har ikke fungert som en effektiv kontrollmekanisme.
- Sentrale informasjonssikkerhetsrisikoer knyttet til ESN-kontrakten har ikke blitt tilstrekkelig vurdert.
- Presentasjonen til styret i Helse Sør-Øst RHF var upresis og varsler om dette ble ikke kommunisert til administrerende direktør i Helse Sør-Øst RHF.

Datatilsynets varsel om vedtak til helseforetakene i Helse Sør-Øst

Datatilsynet henvendte seg i mai 2017 til alle helseforetakene i Helse Sør-Øst RHF. I brevet ba de om en redegjørelse blant annet for hvilke risikovurderinger og aksept av restrisiko som lå til grunn for beslutningen om å tjenesteutsette ansvaret for IKT-drift i regionen (se omtale av PwC-rapporten ovenfor). Det foreligger nå varsel om vedtak til ni av helseforetakene i Helse Sør-Øst hvor det oppgis følgende hovedkonklusjoner:

- De behandlingsansvarlige helseforetakene ikke har hatt tilstrekkelig eierskap til, eller kontroll med de planlagte endringene knyttet til informasjonssystemet.
- Helseforetakene har overlatt ansvaret for beslutninger som har betydning for pasientenes personvern og informasjonssikkerheten knyttet til behandling av personopplysninger, til databehandleren og til ansatte lenger ned i organisasjonen.
- Det ble ikke gjennomført nødvendige risiko- og sårbarhetsvurderinger før det ble besluttet å konkurranseutsette avtale om strategisk partnerskap, herunder drift og vedlikehold av IKT-infrastruktur.
- Det ble heller ikke gjennomført nødvendige risiko og sårbarhetsanalyser i forkant av at det ble besluttet å velge underleverandør i Bulgaria.
- Valgt underleverandør har i et begrenset tidsrom hatt tilgang til pasientopplysninger i strid med ledelsens forutsetning om tilgangskontroll.

Datatilsynet kommenterer at Helseforetakene legger til grunn at det ikke er et krav om at risikovurdering gjennomføres før behandling av personopplysninger iverksettes. Dette er Datatilsynet uenig i. Det kommenteres også at utkontrakteringen, på grunn av sitt omfang, ligger nær opp til eller i grenseland til sikkerhetslovens virkeområde. Datatilsynet vurderer at sikkerhetsloven er

relevant selv om den ikke kommer direkte til anvendelse. Selv om Helseforetakene ikke har definert konsolidering av pasientopplysninger i helseregionen som skjermingsverdig etter sikkerhetsloven, mener Datatilsynet at helseforetakene, som et minimum, burde tatt i betraktning hvordan risikovurderinger utføres i saker som er omfattet av sikkerhetsloven.

Vedtaket gjelder et forhåndsvarsel om overtredelsesgebyr på kr 800.000 til ni helseforetak i Helse Sør-Øst for overtredelser av bestemmelser i person-opplysningsforskriften og pasientjournalloven. Endelig vedtak er ikke fattet i saken.

3.2 Teknologitrender som kan påvirke bruk av private leverandører

Både bruk av og markedet for teknologi er hele tiden under utvikling. Det er flere trender som påvirker hvordan tjenestene kan leveres og som kan endre bruken av private leverandører og deres mulige tilgang til pasientinformasjon.

Eksempler på noen viktige trender er:

- Mer standardløsninger og mer internasjonalt marked.
- Overgang til leveranse som tjenester («skyen»).
- Mer bruk av smidige og andre nye «trinnvise» metoder for programvareutvikling.
- Konsolidering og integrasjon av systemer.
- Tingenes internett og selvbetjening.
- Mer bruk av stordata og kunstig intelligens.
- Globalisering, kompliserte konsernstrukturer og lange leverandørkjeder.

3.2.1 Mer standardløsninger og mer internasjonalt marked

Helse- og omsorgsektoren i Norge bruker i stor grad «standardløsninger» som er utviklet og videreutvikles av norske eller internasjonale private leverandører. Det forventes ikke at denne situasjonen vil endres, men trenden vil heller være at man i enda større grad bruker internasjonale løsninger. Dette medfører at sektoren må forholde seg til internasjonale leverandører og deres leveranse-modeller, samt til løsninger som ikke er utviklet spesielt med tanke på norske lover og regler for informasjonssikkerhet.

Innen medisinsk-teknisk utstyr er man allerede helt avhengig av internasjonale løsninger. Leverandørene tilbyr flere tjenester rundt sine produkter. Det er for eksempel et økende behov og ønske om å gi leverandørene mer fjernaksess til løsninger, for å sikre bedre og mer effektivt vedlikehold og overvåking. Noen tjenester inkludere også lagring av visse data hos leverandøren.

3.2.2 Overgang til leveranse som tjenester («skyen»)

En annen stor trend innen IKT er skytjenester. Skytjenester vil si at virksomheter i stedet for å kjøpe produkter som de selv drifter, så får virksomheten levert dette som standardisert tjeneste over internett driftet av leverandøren. Leveransene gjøres gjerne «globalt». Med personvernforordningen som trer i kraft i 2018 vil også databehandlere utenfor EØS bli underlagt europeisk lovgivning så sant de behandler personopplysninger om innbyggere fra EØS-området.

Skytjenester som begrep blir ofte kategorisert i tre ulike leveransemodeller. Dette er allmenn tilgjengelig, privat og hybrid sky. Allmenn tilgjengelig sky er som oftest standardiserte tjenester som leveres likt til kundene på leverandørens premisser. Privat sky er skytjenester som kun gjøres tilgjengelig for virksomheten og hvor kunden selv ofte kan tilpasse løsningen etter egne behov. Hybridsky vil som oftest være en kombinasjon av de to leveranse-modellene.

Skytjenester er ofte en integrert del av velferdsteknologi på forbrukermarkedet, og er også på vei inn i IKT-løsninger og medisinsk-teknisk utstyr som leveres til tilbydere av helsehjelp.

Digitaliseringsrundskrivet fra Kommunal og moderniseringsdepartementet av 8.9.2017 sier at «Virksomheter som etablerer nye eller oppgraderer eksisterende fagsystemer eller digitale tjenester, eller endrer eller fornyer avtaler knyttet til drift, skal vurdere skytjenester på linje med andre løsninger».

Skytjenester vil derfor i økende grad bli etterspurt i markedet og tilbudt av private leverandører som en kostnadseffektiv tjeneste. Dette vil dekke både enkle velferdsløsninger og større leveranser. Det vil gi nye muligheter, men også stille nye krav til styring, kontroll og risikovurdering rundt håndtering av pasientinformasjon.

3.2.3 Økt krav og rettigheter for pasienter til å få tilgang til informasjon

Ut fra personvernhensyn og på grunn av tekniske forutsetninger, har det historisk vært et mål at personopplysninger lagres og behandles i den enkelte virksomhet. Fokuset går nå mer i retning av at den enkelte person skal ha kontroll på sine opplysninger, samtykke til å bli registrert, informeres om all registrering, og ha rett til innsyn, flytting og sletting. Dette gjenspeiles også i den kommende personvernforordningen.

Med dette utgangspunktet kan personvernet og informasjonssikkerheten bli vel så godt ivaretatt i store profesjonelt drevne fellesløsninger som i små og mange løsninger driftet i virksomhetens lukkede soner. I skyløsninger er det vesentlig enklere å lage innsynsløsninger og andre personvernstjenester for pasienten.

3.2.4 Mer bruk av smidige og andre nye metoder for «trinnvis» programvareutvikling

Innen programvareutvikling og systeminnføring får smidige og trimmede metoder stadig større utbredelse. Med smidige metoder leverer man hyppigere, inkrementelt (trinnvis) og iterativt (repeterende). I både smidige og trimmede metoder foretrekkes tverrfaglige lag og IKT-utviklere og brukere jobber sammen. I sin ytterste konsekvens betyr det at man tar bort skillet mellom dem som arbeider med utvikling og dem som arbeider med drift. Dette kan medføre at private leverandørers personale får mer omfattende tilgang til pasient-informasjon.

3.2.5 Konsolidering og integrasjon

I helse- og omsorgsektoren ser vi en trend mot konsolidering av systemer og mer integrerte systemer for å etablerer felles løsninger og oppnå elektronisk informasjonsutveksling.

Trenden medfører at konsekvensene av brudd på informasjonssikkerhet blir større siden det rammer flere i større omfang. Den medfører også at eksisterende løsninger der infrastrukturen primært har vært sikret ved å skjerme systemene fra utenverdenen blir mer sårbare.

3.2.6 Selvbetjening og velferdsteknologi

Utstyr og løsninger som kommuniserer gjennom internett, tas i bruk av brukeren selv, eller ønskes tatt i bruk innen mange ulike deler av helse- og omsorgs-sektoren, øker i omfang. Dette vil gjelde flere områder med for eksempel selvbetjening innen sektoren.

Velferdsteknologi kan bidra til økt trygghet og bedre tjenester for brukere og pårørende, samt gi en bedre utnyttelse av ressurser i helse- og omsorgs-tjenesten. Men det gir også flere utfordringer sikkerhetsmessig og hva angår ansvarsforhold. Blant leverandørene er det ulik grad av sikkerhetsforståelse. Dette gjelder ikke bare ivaretakelse av konfidensialitet, men også integriteten i dataene, tilgjengelighet og datakvalitet. Dette omtales nærmere som forbedringsområde i kapittel 5. Velferdsteknologi-programmet[21] gir en mer utfyllende beskrivelse av utfordringsbildet.

3.2.7 Stordata og kunstig intelligens

To trender som påvirker bruken av informasjon som finnes i pasientjournaler og helseregistre er stordata og kunstig intelligens. Ny teknologi gjør det mulig å bruke data som tidligere var svært vanskelig tilgjengelige, herunder data fra utlandet, til forskning og beslutningsstøtte for praktikere. Det blir en økende

21 Se flere rapporter på https://helsedirektoratet.no/velferdsteknologi#-rapporter-og-utredninger

interesse for informasjonsdeling på tvers av landegrenser og for private leverandører å få tilgang til pasientinformasjon.

3.2.8 Globalisering, kompliserte konsernstrukturer og lange leverandørkjeder

En annen trend med konsekvenser for informasjonssikkerhet ved tjeneste-utsetting er utviklingen mot globale leverandører med kompliserte konsern-strukturer og lange kjeder med underleverandører som opererer i ulike jurisdiksjoner med ulike regelverk.

Mange leverandører, også norske, benytter internasjonale nettverk av leveranse-sentre. Dette gjør det enklere å kunne tilby tilstrekkeligkapasitet og kompetanse døgnet rundt. Ved å plassere sentrene i ulike tidssoner er det også mulig å la oppgavene «følge solen». Med hele verden som arbeidsfelt blir det lettere å kunne konsentrere seg om noen få arbeidsoppgaver og bygge spiss-kompetanse. I tillegg kommer muligheten for å levere til lavere kostnad fra lavkostland.

Mange leverandører har kompliserte konsernstrukturer og benytter i stor grad underleverandører, og det er utfordrende når eierskapsstrukturen og leverandører som benyttes endrer seg. Risikovurderingen må ta høyde for dette.

Bruk av denne type leveransemodeller fra private leverandører brukes i stor skala i andre bransjer som bank, olje og telekommunikasjon. Slike modeller krever en aktiv risikostyring og kontroll, og ikke minst økt kompetanse i kravstilling og kontraktsoppfølging.

4 Bruk av private leverandører

Innhenting av informasjon

Det er innhentet informasjon om status på bruk av private leverandører fra de aktørene i sektoren som behandler pasientinformasjon; de regionale helseforetakene, fastleger, Helsetjenestenes driftsorganisasjon (HDO), Pasientreiser, Folkehelseinstituttet og Norsk Helsenett. Bortsett fra fastleger er innspill innhentet ved hjelp av både et spørreskjema[22] og dialog. For fastlegene er det avholdt særmøte og involvering av leger som deltar i EPJ-løftet. Det er kun informasjonen som er innhentet skriftlig som danner grunnlag for resultatene.

Informasjonsinnhentingen er rettet mot IKT-løsninger som inneholder pasientinformasjon innenfor følgende tjenesteområder:

- Basisdrift
- Applikasjonsdrift
- Applikasjonsforvaltning
- Applikasjonsutvikling og -innføring

I tillegg har aktørene besvart spørsmål vedrørende tilgang til løsninger, forhold knyttet til medisinsk-teknisk utstyr, samt bruk av skyløsninger.

Presiseringer

For å få en oversikt over tjenesteutsetting innenfor de enkelte tjenesteområdene, er aktørene bedt om å angi hvor stor prosentandel av totalkostnadene for hvert tjenesteområde som brukes på private leverandører. Dette gir nødvendigvis ikke et eksakt bilde på bruk av private leverandører, men en indikasjon på bruken. I tabellene nedenfor er disse prosentandelene brukt som grunnlag for en gradsvurdering på bruk av private leverandører.

Mange av aktørene bruker Norsk Helsenett som driftsleverandør. Norsk Helsenett blir i denne rapporten ikke vurdert som en privat leverandør. Dette medfører at innspill fra aktørene om at de drifter noen tjenester selv, inkluderer bistand fra Norsk Helsenett.

4.1 RHFene

Alle de fire regionale helseforetakene har svart på spørreskjemaet. I tabell 4.1 presenteres en oppsummering på bruk av private leverandører for hvert tjenesteområde (basert på andel kostnader for hvert tjenesteområde).

22 Se vedlegg 4 for en oversikt over alle spørsmålene.

Tabell 4.1: *Bruk av private leverandører på de enkelte tjenesteområdene for RHFene.*

Aktører	Basisdrift	Applikasjons-drift	Applikasjons-forvaltning	Applikasjons-utvikling og -innføring
Helse Sør-Øst	I liten grad	I liten grad	I stor grad	I meget stor grad
Helse Vest	I meget liten grad	I liten grad	I stor grad	I stor grad
Helse Midt	Ingen	I liten grad	I meget stor grad	I meget stor grad
Helse Nord	I liten grad	I liten grad	I meget stor grad	I stor grad

Resultatene som presenteres i tabellen viser at RHFene i stor grad benytter seg av private leverandører på applikasjonsforvaltning, -utvikling og -innføring og i liten grad på basis- og applikasjonsdrift. Noe av forskjellene i tabellen kan skyldes ulik tolking fra de enkelte RHFene gitt at det virker som RHFenes bruk av private leverandører er relativt lik på de ulike områdene.

4.1.1 Vurdering av de enkelte tjenesteområdene

Basis- og applikasjonsdrift

Når det gjelder basis- og applikasjonsdrift håndteres dette for det meste av RHFene selv eller av Norsk Helsenett. Det er relativt liten variasjon på bruk av private leverandører. RHFene oppgir at prosentandelen av totalkostnadene som brukes på private leverandører på basis- og applikasjonsdrift ligger mellom 0–10 prosent. Private leverandører støtter primært på drift av enkelte komponenter og mindre IKT-løsninger.

Aktørene har til nå vært tilbakeholdne med å utkontraktere basisdrift av systemer som inneholder pasientinformasjon til private leverandører. Dette er dels basert på risikovurdering og dels basert på en vurdering av kostnad og kvalitet. Sentrale sikkerhetsfunksjoner som brannmurdrift, overvåkning av infrastruktur, sikkerhets og -sårbarhetsovervåkning av servermiljø, blir av enkelte fremhevet som noe man spesielt ønsker intern kontroll på.

Applikasjonsforvaltning

For alle RHFene gjennomfører private leverandører en betydelig andel arbeid med applikasjonsforvaltningen. Angitt prosentandel av totalkostnader som brukes på private leverandører på applikasjonsforvaltning varierer fra 40 til 90 prosent. Helse Sør-Øst og Helse Vest bruker private leverandører i noe mindre grad enn Helse Midt og Helse Nord på applikasjonsforvaltning.

RHFene påpeker at de har gode rutiner med å begrense private leverandørers tilgang til pasientinformasjon i forbindelse med applikasjonsforvaltning. Det vil allikevel være situasjoner hvor ansatte hos private leverandører får tilgang til pasientinformasjon, for eksempel ved alvorlige feilsituasjoner.

Applikasjonsutvikling og -innføring

For RHFene har private leverandører et stort ansvar innenfor applikasjons-utvikling og -innføring. Angitt prosentandel av totalkostnader på disse tjenesteområdene som går til private leverandører varierer fra 50 til 90 prosent. Helse Nord og Helse Vest ligger noe lavere enn Helse Midt og Helse Sør-Øst. RHFene driver med begrenset egenutvikling, og det er bred enighet mellom RHFene at man må kjøpe de beste norske og internasjonale standardløsningene innen applikasjonsutvikling.

RHFene arbeider bevisst med å minimere tilgangen til pasientinformasjon ved applikasjonsutvikling og innføring av løsninger, men i noen tilfeller må dette gis for å kunne innføre ny løsning og sikre høy kvalitet. Mye av arbeidet med applikasjonsutvikling og -innføring gjøres uten av man trenger eller har tilgang til pasientinformasjon. Leverandørene vil allikevel kunne få tilgang til pasient-informasjon rundt aktiviteter som konvertering av data fra gammel til ny løsning, slutt- og produksjonstester, migrering og produksjonssetting. Disse tjenestene kjøpes som regel i noe omfang fra private leverandører der man har større innføringsprosjekter, som for eksempel innføring av kjernejournal eller andre store fagsystemer.

4.1.2 Andre områder

Ansatte hos private leverandører kan også få tilgang til pasientinformasjon gjennom andre kanaler, ikke minst gjennom medisinsk-teknisk utstyr og skyløsninger.

Medisinsk-teknisk utstyr

Alle RHFene oppgir at leverandører av medisinsk-teknisk utstyr har fjernaksess eller intern aksess til levert utstyr knyttet til overvåking, feilsøking, feilretting, oppgraderinger og generell service og vedlikehold av utstyr og tilhørende programvarer. I noen tilfeller vil dette kunne gi tilgang til pasientinformasjon, men RHFene prøver å begrense dette. RHFene har prosesser, rutiner og sikkerhetsløsninger som de mener håndteres i henhold til kravene.

Noen RHFer påpeker at det er et økende behov og ønske fra leverandørene om fjernaksess for å sikre oppetid og dermed pasientsikkerhet. Det er i tillegg økonomiske fordeler ved bruk av fjernaksess. RHFene nevner også at det er en internasjonal trend at medisinsk-teknisk utstyr i større grad leveres som tjenester og dette kan gi private leverandørene økt tilgang til pasient-informasjon. Så langt har dette i liten grad skjedd i Norge.

Bruk av eksterne skytjenester

Bruk av eksterne skytjenester gjøres i dag i meget begrenset omfang for løsninger med pasientinformasjon. Noen bruker skyløsninger for noen få konkrete løsninger og andre ved bruk av medisinsk-teknisk utstyr.

Flere av RHFene forventer at både behov og ønsker om bruk av skyløsninger raskt vil øke i omfang. Dette er blant annet knyttet til at pasientnære e-helse- og velferdsteknologier øker, og at ved kjøp av medisinsk-teknisk utstyr vil det følge med skybaserte tjenester. Eksempler på dette er oppfølging av kronikere (KOLS, diabetes m.fl.), data fra pacemakere og oppfølging av kreftpasienter hjemme. Pasientene vil i økende grad skaffe seg løsninger som brukes utenfor institusjon, og ønsker at data fra disse løsningene skal brukes i behandlingen gitt av institusjonene.

4.1.3 Hvilke land private leverandører har tilgang fra

Tabellen nedenfor gir en oversikt over hvilke land RHFenes leverandører, og eventuelt underleverandører oppholder seg i.

Tabell 4.2: *Oversikt over hvilke land de private leverandører har tilgang fra.*

Land og områder	Prosentandel (laveste og høyeste pr. RHF)
Norge	60 – 84 %
EU/EØS	14 – 30 %
Andre	2 – 10 %

Når det gjelder «andre» representerer dette primært USA. Det er også tilgang fra Israel, India og andre land i Asia. Noen leverandører leverer tjenester etter «følg solen»-prinsippet, som innebærer at arbeidet forflytter seg mellom ulike tidssoner gjennom døgnet. Helse Vest og Helse Sør-Øst benytter dette i noe omfang i dag.

Resultatene viser at leverandører og underleverandører som har tilgang til pasientinformasjon primært oppholder seg i Norge eller EU/EØS-området. Det er begrenset (to prosent) tilgang utenfor EU/EØS-område.

4.1.4 Betingelser ved bruk av private leverandører

RHFene har regionale sikkerhetssystemer og krav som gir betingelser som må oppfylles for at private leverandører kan få tilgang til pasientinformasjon. Normen og andre regulatoriske krav må oppfylles. Det gjennomføres risikovurderinger for å identifisere hvorvidt tjenesten opererer innenfor et akseptabelt risikonivå.

RHFene understreker at de har styring og oppfølging av fjernaksess til løsningene. Kun autoriserte personer hos leverandørene får tilgang i en begrenset periode. RHFene gjennomfører regelmessige gjennomganger av hvem som har tjenstlige behov for tilgang. I tillegg skal pasientinformasjon ikke hentes ut uten en avtale.

Det inngås databehandleravtaler med leverandører, men noen RHFer påpeker at det kan være utfordrende å sikre rekken med underleverandører.

4.1.5 RHFenes tilfredshet med private leverandører

Generelt er RHFene positive til private leverandører. De har tillit til leverandørene og understreker at de er avhengige av bistanden fra de private leverandørene. Enkelte RHFer har opplevd tilfeller der pasientinformasjon ikke er blitt håndtert i henhold til avtaler eller der det burde ha blitt søkt om samtykke. Ett RHF påpeker at det er stor kompetanseforskjell hos de private leverandørene på informasjonssikkerhet, evne til å etterleve eksisterende personopplysningslov og bransjenorm. Videre mener RHFene at kompetanse innen IKT og forståelse for eksisterende trusler og sårbarheter gjerne er større hos de største leverandørene. Samtidig opplever ett RHF at større leverandører ikke oppleves som like smidige. De private leverandørene ønsker i blant å benytte egne løsninger for fjernaksess, men på grunn av et strengt tilgangsregime så tillates ikke dette.

4.2 Andre som behandler pasientinformasjon

I arbeidet med rapporten er det innhentet informasjon fra andre i sektoren som behandler pasientinformasjon. Disse er Pasientreiser, Folkehelseinstituttet, HDO, Norsk Helsenett og Direktoratet for e-helse. Nedenfor er en oppsummering av den innsamlede informasjonen. Resultatene e inkluderer ikke svar på alle spørsmålene i spørreskjemaet fordi enkelte spørsmål ikke var relevante for noen av aktørene.

I tabell 4.3 presenteres en oppsummering bruk av private leverandører (basert på andel kostnader for hvert tjenesteområde):

Tabell 4.3: *Oversikt over bruk av private leverandører på de enkelte tjenesteområdene for Pasientreiser, Folkehelseinstituttet, HDO, Norsk Helsenett og Direktoratet for e-helse.*

Aktører	Basisdrift/ applikasjonsdrift	Applikasjons-forvaltning	Applikasjonsutvikling og -innføring
Folkehelseinstituttet	Ingen	Ingen	I noen grad
Pasientreiser	Ingen	I meget stor grad	I meget stor grad
HDO	Ingen	I liten grad	Utvikling: Alt Innføring: ingen
Norsk Helsenett	I liten grad	I liten grad	Utvikling: I stor grad Innføring: I liten grad
Direktoratet for e-helse	I noen grad	I noen grad	I stor grad

Når det gjelder basisdrift og applikasjonsdrift er dette i liten grad satt ut til private leverandører, bortsett fra i Direktoratet for e-helse. For applikasjons-

forvaltning er det noe større variasjoner. Noen forvalter dette internt, mens andre har satt nesten alt ut til private leverandører. På applikasjonsutvikling og -innføring gjøres betydelig mer av private leverandører. Alle aktørene opplyser at de benytter seg av privat leverandører innenfor dette tjenesteområde og dette gjelder spesielt på applikasjonsutvikling.

4.2.1 Folkehelseinstituttet

Status

Folkehelseinstituttet gjør stort sett alt på basisdrift, applikasjonsdrift og applikasjonsforvaltning internt. De får noe bistand på applikasjonsutvikling og -innføring og angir at 15 prosent av totalkostnadene på applikasjonsutvikling og -innføring brukes på private leverandører. Folkehelseinstituttet understreker at private leverandører i liten grad får tilgang til pasientinformasjon.

Folkehelseinstituttet bruker ikke private skyløsninger. Når det gjelder medisinsk-teknisk utstyr har leverandørene ikke fjernaksess til dette, men ved behov kan leverandøren arbeide ved fysisk fremmøte i samarbeid med Folkehelse-instituttets medarbeidere.

Leverandørens personale som kan få tilgang til pasientinformasjon kommer stort fra Norge og alle innen EØS/EU-område. Teoretisk kan personer utover EØS få tilgang.

4.2.2 Pasientreiser

Status

Pasientreiser utfører selv basis- og applikasjonsdrift. Når det gjelder applikasjonsforvaltning, -utvikling og -innføring utføres det meste av private leverandører. Pasientreiser angir at private leverandører har svært stor tilgang til pasientinformasjon. Dette skyldes at de følger en smidig utviklingsmetode som forutsetter innsyn i pasientinformasjon.

Pasientreiser benytter i dag ingen skytjenester hvor det behandles pasient-informasjon, og de har ikke medisinsk-teknisk utstyr. De private leverandørene kommer stort sett fra Norge og noe fra EØS/EU.

Erfaring leverandører

Pasientreiser har stort sett positive erfaringer med sine leverandører, og leverandørene har rett holdning til personvern og informasjonssikkerhet.

Betingelser

Når det gjelder sikring av pasientinformasjon ved bruk av private leverandører, vurderer Pasientreiser ved hvert enkelt tilfelle hvorvidt det er behov for å benytte pasientinformasjon. Tilganger styres også ut fra behov og vil ta utgangspunkt i arkitekturprinsipper, Normen, taushetserklæringer og databehandleravtale.

4.2.3 Helsetjenestens driftsorganisasjon (HDO)

Status

HDO drifter selv basis- og applikasjonsdrift. Når det gjelder applikasjonsforvaltning får de noe bistand fra private leverandører på Nødnett, angitt til 10 prosent av totalkostnadene på tjenesteområdet. Når det gjelder applikasjonsforvaltning på lydlogg gjøres alt arbeidet av HDO. All applikasjonsutvikling gjøres av private leverandører, men selve innføringen gjøres av HDO. Private leverandører har ingen tilgang til pasientinformasjon. Lydlogg er den eneste applikasjonen som har pasientinformasjon og den forvalter og drifter HDO selv. Nødnett inneholder ikke pasientinformasjon.

HDO verken drifter eller forvalter medisinsk-teknisk utstyr, og de benytter heller ikke skytjenester hvor det behandles pasientinformasjon.

Erfaring med private leverandører

HDO har meget positive erfaringer med leverandørene av Nødnett og tilstøtende applikasjoner. Det er ikke avdekket avvik vedrørende de retningslinjene som er avtalt mellom partene. Det er ingen leverandører som har tilgang til Lydlogg, som er eneste applikasjonen HDO drifter og forvalter som inneholder pasientinformasjon.

Betingelser

I anskaffelsesprosessen blir leverandører bedt om å signere på databehandleravtale. Der enkeltpersoner skal inn i systemene, signeres taushetserklæring. Etter innføring og før overføring til drift sletter HDO alle brukere som ikke tilhører HDO drift.

4.2.4 Norsk Helsenett

Status

Norsk Helsenett står selv for mye av basisdrift, applikasjonsdrift og applikasjonsforvaltning og angir at 5 prosent gjøres av private leverandører. På applikasjonsutvikling står private leverandører for en større andel, anslått til noe under 50 prosent av totalkostnadene. Applikasjonsinnføring gjør de stort sett selv. Bistanden fra private leverandører er anslått til under 5 prosent av totalkostnadene. Norsk Helsenett mener at private leverandører i liten grad har tilgang til pasientinformasjon. Dette gjelder kun i noen få tjenester der databehandlingsansvarlig benytter private underleverandører i tillegg til Norsk Helsenett som driftsleverandør. Norsk Helsenett har ingen skytjenester hvor det behandles pasientinformasjon og har ikke ansvar for medisinsk-teknisk utstyr. I dag holder all personell som arbeider med pasientinformasjon til i Norge og Norsk Helsenett har ingen avtale med utenlandske leverandører knyttet til slik drift.

Erfaring med private leverandører

Vedrørende erfaring med private leverandører mener Norsk Helsenett at det ofte er utfordringer knyttet til det å ha god nok oversikt over tilganger. For enkelte tjenester er det forventet at man driver utvikling som krever flere underleverandører og hyppige leveranser. Dette har til tider vært utfordrende med tanke på kontroll.

Betingelse

Norsk helsenett benytter private leverandører i svært beskjeden grad inn mot helse- og personopplysninger. De understreker at hvilke kriterier man velger å sette avhenger av systemet, men kompetanse og evnen til å forholde seg til norsk lovverk har stor oppmerksomhet.

Norsk Helsenett krever alltid at leverandører skal følge kravene i Normen. Dersom dette ikke er mulig, må de private leverandørene forplikte seg til EU/EØS-lovgivning.

En del av Norsk Helsenetts virksomhet er å legge til rette for at brukerne av Helsenettet skal få tilgang til nyttige og relevante tjenester. En del av tjenestene leveres av ca. 200 godkjente, eksterne leverandører som tilknyttes Helsenettet. Dette omfatter:

- Driftsleverandører – ASP
- Driftsleverandører – Fjerndrift
- Journalleverandører
- Regnskap og betalingsløsninger
- Back-up
- Telefoni/videoløsninger
- Andre tjenester som frankeringsmaskiner, talegjenkjenning, sertifikathåndtering og lignende tjenester.

En rekke av leverandørene som tilknyttes Helsenettet ønsker å informere om sine tjenester på nhn.no. Det finnes en oversikt over disse her: https://nhn.no/tredjepartsleverandoerer/

4.2.5 Direktoratet for e-helse

Direktoratet for e-helse står selv (gjennom Norsk Helsenett) for mye av basis- og applikasjonsdrift, men bruker private leverandører i et visst omfang (angitt til 25 prosent av totalkostnader på tjenesteområdene). På applikasjonsforvaltning, -utvikling og -innføring brukes det private leverandører i større grad (angitt til 40 prosent av totalkostnadene på tjenesteområdene).

I dag holder alt personell som arbeider med pasientinformasjon for Direktoratet for e-helse til i Norge.

4.2.6 Private fastleger

Informasjon om fastlegers løsninger og bruk av private leverandører er innhentet ved kontakt med fastleger som er en del EPJ-løftet og fra Direktoratet for e-helse sitt arbeid med prosjekt for «Digital dialog med fastleger». Det finnes ingen samlet oversikt over løsninger og bruk av private leverandører, men det antas at den informasjonen som er samlet inn gir et tilstrekkelig bilde av situasjonen, med tanke på sikkerhetsmessige utfordringer.

Private leverandører tilbyr i dag følgende primære tjenester til fastlegene:

- Basisdrift inkludert applikasjonsdrift
- EPJ-løsninger – utvikling og forvaltning
- Medisinsk-teknisk utstyr, inkludert oppkobling og feilretting
- Betalingsløsninger

Noen private fastleger bruker kommunens IKT-løsninger, men omfanget er ikke kartlagt.

Nedenfor er det oppsummering av status når det gjelder privat leverandører knyttet til de ulike områdene.

Basisdrift inkludert applikasjonsdrift

Fastlegenes bruker i dag ulike alternativer for basis- og applikasjonsdrift. Det opplyses om fire alternativer:

1. Lokal drift utført av eget personale. Løsningene er installert på en server på det lokale legekontoret og driftes av personale på legekontoret.
2. Lokal drift, men med viss bistand fra ekstern private leverandører. Løsningene er installert på en server på de lokale legekontoret. Private leverandører bistår i større eller mindre grad med driften av løsningene. Leverandørene kan være mindre lokale firmaer eller kjente. Bistanden ytes enten via fjernaksess eller fysisk oppmøte på kontoret.
3. Lokalt, men legekontoret har en totalleverandør. Løsningen er installert på en server på legekontoret, men legekontoret har en leverandør som tar totalansvar for driften.
4. Fjernleverandør av driftstjenester. Løsningene er installert hos leverandør som har ansvar for drift av løsningene. Legekontoret har fjernaksess til sine løsninger og det vil si ingen lokal installasjon.

For alternativ 2, 3 og 4 vil den private leverandøren ha stor tilgang til pasientinformasjon.

Applikasjonsforvaltning, -utvikling og -innføring av løsninger

Det er primært tre private leverandører av EPJ-løsninger til legekontorer/fastleger i Norge. Disse leverandørene utvikler løsningene og bistår med innføring og forvaltning av løsningene. Noe av forvaltningen gjøres av personale

på det enkelte legekontor, som installasjon av mindre oppdateringer og fikser. Leverandørene av EPJ-løsningen vil under arbeidet ha tilgang til løsningene via fjernaksess eller ved lokalt oppmøte, og dermed tilgang til pasientinformasjon.

Løsningene installeres på legekontorets server eller datasenter som leverer driftstjenester. Det er kommet en ny skybasert EPJ-løsning, men denne har ikke stor utbredelse. De etablerte leverdørene synes å følge utviklingen av sky-tjenester og har allerede tilbud om, eller er på vei til å komme med tilbud om, skyløsning/hosting for sine løsninger. Noen leger er skeptiske til skyløsninger og begrunner dette primært med usikkerhet vedrørende tilgjengelighet

I tillegg har legekontorer også betalingsløsninger hvor leverandøren av disse også har tilgang til en viss pasientinformasjon, for eksempel hvilke tjenester pasientene har betalt for.

Når det gjelder kvalitetssystemer, opplyses det om at mellom 30 og 40 prosent av fastlegekontorene benytter seg av TrinnVis kvalitetssystem. TrinnVis er et nettbasert styrings- og kvalitetssystem som gir en oversikt over samarbeids-partnere som har tilgang til lokaler og datasystem.

Medisinsk-teknisk utstyr

Fastlegekontorer har medisinsk-teknisk utstyr som både kan være frittstående og tilknyttet PC. Vanligvis er det private leverandører som installerer utstyret og driver med oppdateringer eller feilretting. Leverandørene har vanligvis ikke fjernaksess. Leverandørene vil under arbeidet ha tilgang til server der pasient-informasjon er lagret og kan få innsyn i pasientinformasjon som er lagret i medisinsk-teknisk utstyr. Leverandører har i prinsippet ikke tilgang til annen pasientinformasjon, men kan gjennom sin tilgang til serveren ta kopi av data som er lagret på denne.

Oppsummering

Hos de aller fleste fastleger er det en eller flere private leverandører som har stor tilgang til pasientinformasjon. Dette gjelder alltid EPJ-leverandøren, men i mange tilfeller også de som bistår på drift eller drifter løsningen. Bistanden gjøres fra Norge, selv om selskapene er utenlandske.

Under hvilke betingelser gis private leverandører tilgang?

Fastlegene prøver å etterfølge Normen, men den kan være kompleks og vanskelig å forstå. Fastlegene inngår databehandleravtale med leverandørene. Leverandøren har egne brukernavn og passord, men kan i noen tilfeller bruke ansattes brukernavn og passord.

I noen tilfeller må leverandøren gjøre vedlikeholdsarbeidet fysisk på lege-kontoret. Dette mener legene gir en ekstra sikkerhet.

Utfordringer med bruk av private leverandører

Utfordringene med bruk av private leverandører relatert til sikkerhet rundt pasientinformasjon, er at man må gi leverandørene tilgang til løsningen og det er ikke enkelt å følge opp hva de enkelte leverandørene gjør. Det er også begrenset kompetanse på det enkelte legekontor. Fordelen med de lokale løsningene man har i dag, er at det er begrenset hvor mye informasjon som kan komme på avveie sammenlignet med en sentral løsning.

4.2.7 Kommuner

Som nevnt innledningsvis skulle kommunesektoren i utgangspunktet være en del av oppdraget. Direktoratet for e-helse sendte ut spørreskjemaet til et utvalg av kommuner, men det har ikke kommet inn tilstrekkelig antall svar for å danne et godt nok grunnlag for å besvare oppdraget fra HOD. Rapporten omhandler derfor ikke kommunesektoren, med unntak av begrenset informasjon om løsninger hos fastleger. Kommunesektoren må eventuelt gjennomgås i en videreføring av prosessen.

5 Hvilke tjenester bør ikke overlates til private leverandører?

Aktørenes vurdering på bruk av private leverandører, er besvart fra samtlige aktører, bortsett fra Sykehusinnkjøp. Aktørene har besvart spørsmålene med ulik grad av detaljeringsnivå. Det er kun den skriftlige, innhentede informasjonen som danner grunnlag for resultatene. Direktoratet for e-helse har i kapittel 5.2 kommet med sin vurdering.

5.1 Resultatene fra aktørene

På spørsmålet om det er noen tjenester som ikke bør settes ut til private leverandører, fikk aktørene mulighet til å svare på dette for hvert tjenesteområde.

5.1.1 Basisdrift

I tabell 5.1 er det en oppsummering av hva aktørene mener ikke bør overlates til private leverandører vedrørende basisdrift.[23] Noen aktører svarer i større grad på hvilke tjenester som er satt ut i dag enn vurderinger av hva som bør eller kan settes ut til private leverandører. Der det i tabellen står «ikke settes ut» menes at private leverandører ikke bør overta dette, uansett jurisdiksjon.

23 Dette er en oppsummering av svar, og ikke ordrette sitater. Innspillene fra hovedaktørene finnes i vedlegg 6, og alle innspillene fra fag- og pasientorganisasjoner finnes i vedlegg 9.

Tabell 5.1: *Oppsummering av svarene fra aktørene på spørsmålet om hvorvidt basisdrift bør overlates til private leverandører.*

Aktørene	Basisdrift	Kommentar
RHFene		
Helse Sør-Øst	Det pågår for tiden en intern prosess i Helse Sør-Øst vedrørende utsettelse av basisdrift, og av den grunn kan ikke dette besvares nå.	
Helse Vest	Ikke satt ut i dag. Visse funksjoner bør ikke settes ut, som for eksempel sikkerhetsfunksjoner.	Beholdt det internt etter en kost- og kvalitetsvurdering. Når det gjelder jurisdiksjoner så har de ikke satt klare begrensninger, men dette må vurderes fra sak til sak. Enklest dersom data er i Norge med, alternativt EU/EØS.
Helse Midt	Ikke satt ut i dag. Kan vurderes under gitte forutsetninger (informasjonssikkerhet, kvalitet og kost).	Ny leverandørstrategi kommer høsten 2017.
Helse Nord	Helse Nord har ikke satt ut basisdrift i dag, og det foreligger ingen planer om å vurdere utsetting av hele eller deler av basisdriften.	Har ellers vurderinger rundt risiko med å sette dette ut til utlandet, og spesielt utenfor EU/EØS.
Andre i sektoren		
Folkehelseinstituttet	Ikke settes ut.	
Norsk Helsenett	Kan bruke private leverandører der det er formålstjenlig gitt at lovkrav oppfylles.	
Pasientreiser	Ikke vurdert dette.	
HDO	Ikke kommentert.	
Fag- og pasient-organisasjoner		
Fagforbundet	Ikke settes ut.	Fagforbundet mener også at IKT-infrastruktur i helsevesenet bør omfattes av sikkerhetslovens regler om håndtering av samfunnskritisk informasjon.
NITO	Ikke settes ut (i dag).	Nåværende infrastruktur for sårbar til å overlates til private. Er deler av dette skjermingsverdig objekt etter sikkerhetsloven?

Aktørene	Basisdrift	Kommentar
Tekna	Ikke sette ut til utlandet dersom det faller inn under kritisk infrastruktur. Kan settes ut til private leverandører som drifter løsning i Norge.	NSM har en klar rådgivende funksjon når det gjelder sikkerhets- og sårbarhetsvurderinger. NSM må ha myndighet til å beslutte om risikoen er større enn forsvarlig nivå, og dermed pålegge at tjenesten ikke kan utkontrakteres.
Den norske legeforening	Bør driftes innenfor landets grenser.	Tillitsforhold til helsedata er viktig. Dette kan bli svekket dersom det driftes i utlandet. IKT i helsetjenesten er samfunnskritisk infrastruktur, noe som betyr at nasjonen må ha nok kompetanse til å håndtere ulike typer hendelser og angrep på denne infrastrukturen.
IKT-næringen		
DXC	Mener alt kan settes ut gitt riktig kontroll og risikovurdering	Bruke en kombinasjon av løsninger som driftes i Norge og utlandet, inkludert skyløsninger.
IBM	Ikke konkludert. Sikkerhetsmuligheter og regulatoriske krav avgjør	For kort tid for kvalifisert svar. Mener man må skille på jurisdiksjon. Løsning med personinformasjon bør muligens håndteres innenfor EU/ EØS.
Sopra Steria	Mener alt kan sette ut, men skille på ulike jurisdiksjoner hvor data kan lagres	De viser til sikkerhetsloven og Lysneutvalget.

Når det gjelder å skille på jurisdiksjon har, som det fremgår av tabellen ovenfor, en rekke aktører kommentert dette:

- **RHFene** har ulike vurderinger knyttet til land og jurisdiksjoner. Dette dekker blant annet forholdet med hva som kan settes ut i Norge, EU/EØS og utenfor EU/EØS.
- **Tekna** mener at det ikke kan settes ut til utlandet, det vil si at det må driftes fra Norge.
- **DXC** mener at det er mulig med en kombinasjon mellom Norge og utlandet.
- **IBM** mener det må skilles på krav mellom Norge, Norden, EU/EØS og andre deler av verden.
- **Sopra Steria** mener at alt kan settes ut, men det må skilles på hvor ulik data kan lagres.

For øvrig viser vi til mer utfyllende kommentarer vedrørende jurisdiksjoner i vedlegg 8.

Oppsummering

Basert på de innkommende svarene så kan det konkluderes med at det er ulike meninger blant aktørene på hvorvidt basisdrift bør settes ut til private leverandører eller ikke.

RHFene kommenterer delvis ut fra nåværende status hvor de har valgt å gjøre det internt, mens ett RHF arbeider med en avklaring. På fagforeningssiden varierer det fra at basisdrift ikke kan settes ut overhode til at det ikke kan settes ut til utlandet. Noen aktører mener denne tjenesteutsettingen bør vurderes i henhold til sikkerhetsloven. Legeforeningen mener det ikke bør settes ut til utlandet, mens IKT-leverandørene heller mot at alt kan settes ut. Noen IKT-leverandører mener at det er behov for mer tid på dette spørsmålet for i bedre grad konkludere med hva som kan settes ut og hvor det kan settes ut.

5.1.2 Applikasjonsdrift, -forvaltning og -utvikling

I tabell 5.2 gis en oversikt over de svarene på spørsmålet om de ulike tjenesteområdene innenfor applikasjoner kan overlates til private leverandører.[24]

Tabell 5.2: *Oppsummering av svar fra hovedaktørene om hvorvidt ulike applikasjonstjenester kan overlates til private leverandører.*

Aktører	Applikasjoner (drift, forvaltning, utvikling og innføring)
Helse Sør-Øst	Applikasjonsdrift og -forvaltning: Drifts- og forvaltningsoppgaver for disse områdene er i all hovedsak i egen regi. Dette ligger tett opp mot Helse Sør-Østs kjerneoppgaver, og det er derfor ikke planlagt endringer i dette. De systemene som brukes er likevel i all hovedsak levert av private leverandører, og disse private leverandørene leverer feilrettinger, oppgraderinger osv. og samarbeider med Helse Sør-Øst i driftssettingen av disse, for eksempel som tredjelinjesupport e.l. Det er derfor behov for betydelig bistand fra private leverandører og deres underleverandører. Det planlegges ikke endringer i denne organiseringen av arbeidet. Applikasjonsutvikling og innføring: Helse Sør-Øst er lite involvert i leverandørenes utvikling (annet enn ev. som bestiller), men innføring foregår i nært samarbeid med private leverandører. Leverandørene av både de systemene som erstattes og de nye vi setter i drift er stort sett private. Disse leverandørene utvikler altså stort sett selv sine løsninger, mens driftssetting inklusive migrering etc. skjer i tett samarbeid med dem. Det planlegges ikke endringer i denne organiseringen av arbeidet.

24 Dette er en oppsummering av svar, og ikke ordrette sitater. Innspillene fra hovedaktørene på dette spørsmålet finnes i vedlegg 6.

Aktører	Applikasjoner (drift, forvaltning, utvikling og innføring)
Helse Vest	Applikasjonsdrift: Hovedregelen er å forestå drift i egen regi og i egne lokaler. Samtidig er det åpning for andre driftsmodeller i anbudsprosesser. Applikasjonsforvaltning, -utvikling og -innføring: Kan settes ut til private leverandører, men Helse Vest har vurdert at det er noen tjenester som ikke bør settes ut (sentrale sikkerhetsfunksjoner).
Helse Midt	Applikasjonsdrift: Daglige drift av applikasjonen gjøres internt, og benytter leverandørmarkedet for feilretting i applikasjonene der dette ikke kan gjøres i egen regi. Applikasjonsforvaltning, -utvikling og -innføring: Bruker i hovedsak leverandørmarkedet for utvikling og videreutvikling av applikasjoner. Står selv for innføring og produksjonssetting.
Helse Nord	Applikasjonsdrift: I liten grad satt ut applikasjonsdrift i dag, og det foreligger ingen planer om å vurdere ytterligere utsetting av hele eller deler av applikasjonsdriften. Applikasjonsforvaltning, -utvikling og -innføring; Dette kan i utgangspunktet settes ut private leverandører, men leverandører som befinner seg i andre land og kontinenter reiser en rekker sikkerhet- og beredskapsutfordringer ikke minst dersom det er utenfor EU/EØS. Bruken av utenlandske leverandører bør derfor vurderes konkret pr. tilfelle.
Norsk Helsenett	Kan bruke private leverandører der det er formålstjenlig gitt at lovkrav oppfylles. Bruker i liten grad private leverandører i dag innenfor disse tjenesteområdene, bortsett fra på applikasjonsutvikling.
Folkehelse-instituttet	Kan settes ut, men avhenger av løsningene.
Pasientreiser	Ingen generell vurdering på dette, men forvaltning, utvikling og innføring gjøres nesten bare av private leverandører
HDO	Ikke svart. Gjør mye av arbeidet med forvaltning og innføring selv. Applikasjonsutvikling gjøres av private leverandører.

Utover hovedaktørene er det primært IKT-leverandørene som har kommentert på bruk av private leverandører for applikasjoner. De mener, i likhet med utsetting av basisdrift, at tjenester vedrørende applikasjoner kan settes ut til private leverandører.

Konklusjonen, når det gjelder applikasjonssiden, er at samtlige aktører mener at mye av arbeidet bør og må gjøres av private leverandører. Dette gjelder applikasjonsforvaltning i noe mindre grad enn applikasjonsutvikling og -innføring. Hovedansvaret og visse funksjoner som driftssetting og sikkerhetsløsninger bør ikke settes ut. De aller fleste aktørene har en strategi som innebærer at det kjøpes standardløsninger der det er mulig.

5.1.3 Innspill fra kompetansemiljøene

Fra kompetansemiljøene er det Nasjonal sikkerhetsmyndighet og Difi som har svart på spørsmålet.

Nasjonal sikkerhetsmyndighet

Generelt om tjenesteutsetting av IKT-tjenester har Nasjonal sikkerhetsmyndighet følgende råd:

- Tjenesteutsetting av IKT-tjenester til profesjonelle aktører vil kunne gi bedre sikkerhet og mer stabile og tilgjengelige tjenester, lavere og mer forutsigbare kostnader og i større grad bidra til bedre fokus om virksomhetens kjerneaktivitet.
- Tjenesteutsetting medfører økt sikkerhetsrisiko på grunn av redusert kontroll på stadig mer komplekse verdikjeder. Virksomheter må aktivt etablere organisatoriske, prosessuelle, tekniske og juridiske sikringstiltak.
- Tjenesteutsetting krever gode risikovurderinger og høy bestillerkompetanse.
- Nasjonal sikkerhetsmyndighet er bekymret for at konsolidering av store mengder nasjonale data ikke gjennomføres med nødvendig verdi- og risikovurdering.

En risikovurdering med hensyn på sikring bør bygge på en verdivurdering, en trusselvurdering og en sårbarhetsvurdering. Sammenstillingen av disse bestemmer risikobildet. Verdivurderingen skal identifisere hvilke verdier som er de viktigste for virksomhetens oppdrag og leveranser, konsekvenser ved tap, avhengigheter med mer. Spørsmål om kritikalitet hører hjemme her. Dette er nærmere beskrevet i «Håndbok: Risikovurdering for sikring».[25]

Direktorat for forvaltning og IKT (Difi)

Difis innspill er at det i henhold til anskaffelsesregelverket i utgangspunktet er liten mulighet til å skille mellom norske leverandører og leverandører fra EU/EØS-området. Unntaket er «rikets sikkerhet» – i praksis betyr det informasjon og systemer hvor sikkerhetsloven kommer til anvendelse.

5.2 Direktoratet for e-helse sin vurdering

Direktoratet for e-helse viser til stortingsmelding nr. 38 (2016–2017) IKT-sikkerhet – Et felles ansvar: «Tjenesteutsetting av IKT-tjenester til profesjonelle aktører vil kunne gi bedre sikkerhet og mer stabile og tilgjengelige tjenester. Det kan også gi lavere og mer forutsigbare kostnader og bidra til bedre prioritering av virksomhetens kjerneområder. Dette fordrer at virksomheten besitter kompetanse til å følge opp leverandører de setter ut tjenester til. Samtidig må virksomheten være bevisst hvilke verdier som eksponeres ved tjenesteutsetting, og iverksette nødvendige tiltak. Behovet for konfidensialitet, integritet og

25 https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/risikovurdering-handbok/

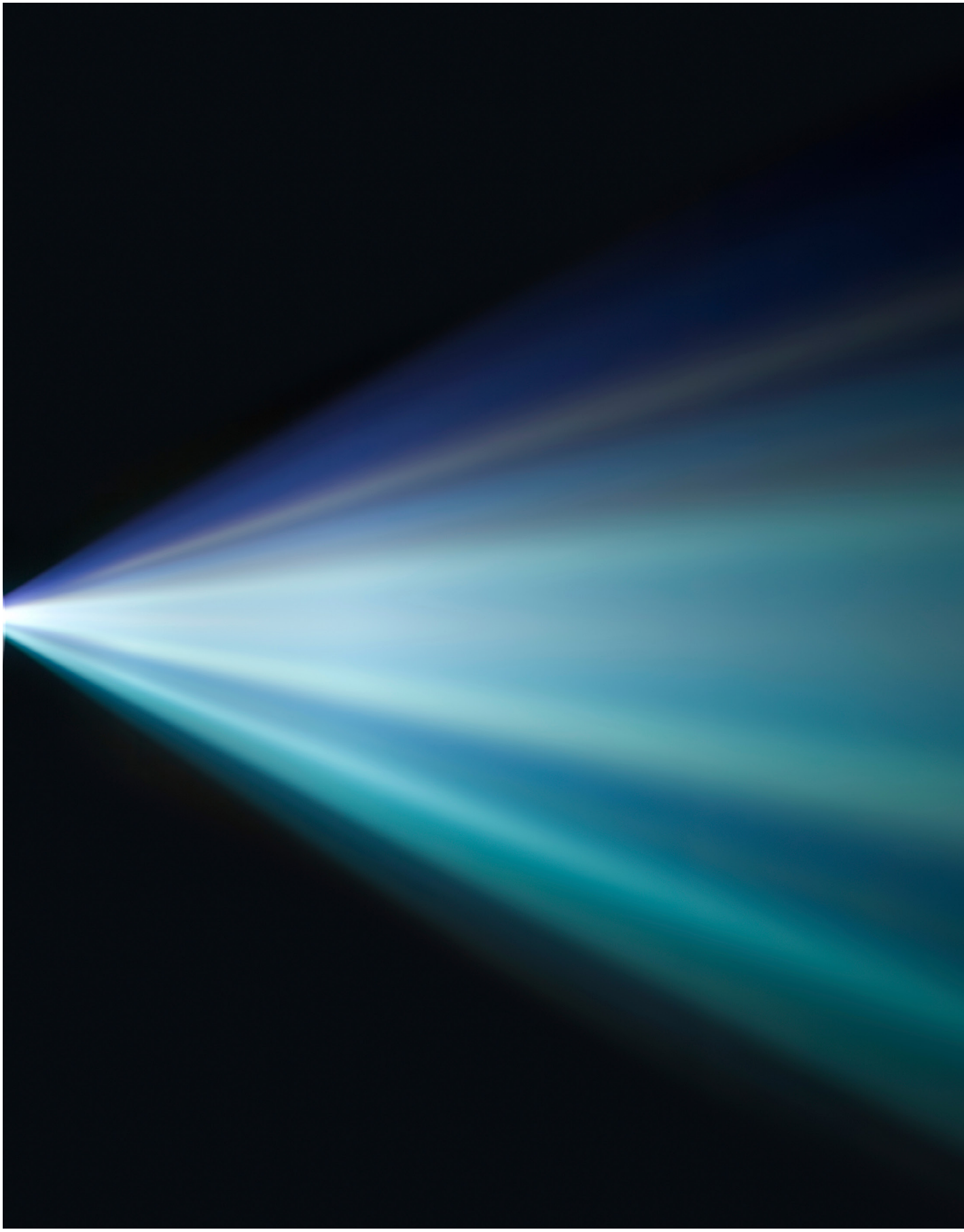
tilgjengelighet bør særlig vektlegges i vurderingene. I tillegg hvilke lover, krav og regler som gjelder for sektoren nasjonalt og internasjonalt».

Direktoratet for e-helse deler oppfatningen som fremkommer i stortingsmeldingen. Basert på dette og arbeidet i rapporten mener direktoratet at det ikke er grunnlag for å konkludere med at noen typer tjenester aldri kan overlates til private leverandører. Det må alltid foretas en risikovurdering av alle tjenester som kan gi tilgang til pasientinformasjon, og en rekke kriterier må være tilfredsstilt på et tilstrekkelig nivå.

Direktoratet for e-helse mener at helse- og omsorgssektoren generelt må ha en relativt lav risikoappetitt, også lavere enn i mange andre bransjer. Tillit fra innbyggerne til at helse- og omsorgssektoren behandler helseopplysninger på en sikker måte, er en forutsetning for å lykkes med digitalisering. Andre forhold som bør påvirke risikoappetitten er at det generelt er høy IKT-kompleksitet i sektoren og at det behandles store mengder sensitive personopplysninger. Flere virksomheter i sektoren har komplekse og gamle løsninger der tekniske sikkerhetstiltak er utfordrende å implementere. Det er viktig at man tar høyde for slike forhold i risikoanalyser og vurderinger av hva man setter ut til private leverandører. Risikoanalyser må også inkludere vurdering av virksomhetens egen bestillerkompetanse.

Direktoratet for e-helse mener at man ved vurdering av land skal gjøre en grundig landrisikovurdering, og spesielt gjelder dette for land utenfor EU/EØS-området hvor særskilte krav må oppfylles. Det anbefales at landrisikovurderingen dekker forhold som er relevante for den enkelte sak og at den også omfatter forhold som for eksempel det konkrete miljøet og kulturen hos tjenesteyter.

Risikovurdering og varsling etter sikkerhetsloven § 29 a om kritisk infrastruktur må gjennomføres der det er relevant, og må i alle tilfeller vurderes ved større IKT-prosjekter.



6 Kriterier og rutiner for bruk av private leverandører

Det eksisterer en rekke rutiner og kriterier for bruk av private leverandører i helse- og omsorgssektoren. Disse er beskrevet blant annet i Norm for informasjonssikkerhet i helse- og omsorgstjenesten (Normen) med faktaark og veiledere, de regionale helseforetakenes styringssystem for informasjonssikkerhet har beskrevne rutiner og lokale prosessbeskrivelser.

Direktoratet har forespurt aktørene i sektoren om anvendelse av nåværende rutiner og forslag til endringer og forbedringer knyttet til bruk av private leverandører, og om det er spesielle kriterier eller betingelser som settes i dag eller foreslås. Direktoratet har også fått innspill fra andre sektorer i dette arbeidet. Direktoratet har i tillegg utarbeidet forslag til kriterier og rutiner med utgangspunkt i egen kompetanse.

Gjennom arbeidet er det avdekket en del forbedringsområder. I kapittel 6.2 er det beskrevet kriterier og rutiner som virksomhetene i sektoren selv må jobbe med, mens i kapittel 6.3 er det beskrevet noen konkrete forbedringsområder hvor gjennomføringsarbeidet bør legges sentralt. Forslagene er ikke fullstendige, og det anbefales å arbeide videre med flere av områdene. Direktoratet for e-helse ser at noen av tiltakene og rutinene som foreslås vil være utfordrende å innføre for mindre virksomheter med begrenset kompetanse på området. Det foreslås tiltak som vil kunne forenkle arbeidet for mindre virksomheter som videreutvikling av Normen og forenkling av vurderingen av sikkerheten ved valg av private leverandører.

Det gjøres også mye bra arbeid innen flere av de forbedringsområdene som omtales, og noen virksomheter i sektoren har kommer lengre enn andre for eksempel med etablering av styringssystemer.

6.1 Dagens status

Dette kapittelet dekker en kort oppsummering av aktørenes innspill på dagens status generelt og på noen spesielle områder, samt en kort presentasjon av Normens krav og veiledningsmateriale.

6.1.1 Generelt

Aktørenes tilbakemelding er at private leverandører benyttes der dette anses formålstjenlig ut fra en vurdering av tilgjengelig kompetanse, kapasitet og kostnad. Valg av leverandører baserer seg på regelverk for offentlige anskaffelser. Det utarbeides kravspesifikasjoner tilpasset hvert system og tjeneste og tildelingskriterier vektes fra gang til gang. Kompetanse og hvilke

avtaler det er mulig å inngå med leverandør, veier gjerne tungt ved anskaffelser. Aktørene understreker at betingelsene i en anskaffelsesprosess varierer på bakgrunn av muligheter i markedet (teknologi og leverandører), hvilket system eller løsning som skal anskaffes og resultatet av gjennomførte risikovurderinger. I tillegg til kompetanse, kostnadseffektivitet og høy kvalitet, nevner flere aktører at private leverandører må ha kunnskap og erfaring med norsk lovverk.

Aktørene oppgir gjennomgående at de følger Normen, samt de rutiner og kriterier som er satt i regionale og lokale styringssystemer.

6.1.2 Norm for informasjonssikkerhet i helse- og omsorgstjenesten (Normen)

Som nevnt ovenfor angir mange aktører at de bruker Normen ved anskaffelse og hovedaktørene oppgir at de bruker den aktivt.

Normen er en bransjenorm for informasjonssikkerhet som forvaltes av sektoren selv gjennom en bredt sammensatt styringsgruppe. Den er utarbeidet av representanter for helse- omsorgssektoren. De omforente reglene i Normen bidrar til at virksomhetene kan ha gjensidig tillit til at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå. Normen stiller krav som detaljerer og supplerer gjeldende lover og forskrifter, men er ikke heldekkende. Helseregisterloven, personopplysningsloven og øvrig regelverk stiller enkelte krav til behandling av helse- og personopplysninger utover det som er tema for Normen.

Sekretariatsfunksjonen for Normen er lagt til Direktoratet for e-helse med deltakelse fra Norsk Helsenett. Det er utarbeidet en stor mengde veiledningsmateriell og kursopplegg basert på Normen. Normen med støttedokumenter vil bli oppdatert som følge av ny personopplysningslov som innfører EUs personvernforordning.

Følgende er de mest relevante veiledere og faktaark til Normen for å få på plass god informasjonssikkerhet ved bruk av private leverandører:

- Faktaark 6b – Sjekkliste for sikkerhetsrevisjon
- Faktaark 10 – Bruk av databehandler
- Faktaark 38 – Sikkerhetskrav for systemer
- Faktaark 46 – Databehandlingsansvar og avtaler i forbindelse med tjenesteutsetting (Målgruppe er kommuner)
- Veileder i bruk av skytjenester til behandling av helse- og personopplysninger
- Veileder for fjernaksess

6.1.3 Flere aktører har egne sikkerhetskrav

Flere aktører viser til at de har egne sikkerhetskrav som leverandør må oppfylle. Leverandørens løsninger må ha en godkjent risikovurdering som blant annet er basert på besvarelsen fra leverandøren. Av relevante standarder som kan ligge til grunn for egne sikkerhetskrav, nevnes for eksempel ISO27001/27002. Sikkerhetskravene er gjerne en integrert del av kravspesifikasjoner som brukes ved anskaffelser.

Leverandørmarkedet peker på at det i dag brukes mye tid på å svare på krav til informasjonssikkerhet og å bli enige om databehandlingsavtaler. Det oppleves at det er stor variasjon i hvilke krav som fremsettes og hvordan de forstås.

6.1.4 Gjennomføring av risikovurdering

Aktørene i sektoren oppgir at det gjennomføres risikovurderinger som et sentralt element ved anskaffelse og innføring av nye løsninger og tjenester. Nivået på risikoanalysene varier ut fra aktørenes størrelse og kompetanse, samt anskaffelsens omfang og innhold.

Dersom tjenesteutsettingen medfører at leverandøren trenger tilgang til pasient-informasjon, gjennomfører aktørene risikovurderinger knyttet til dette og inngår databehandleravtale før databehandling kan starte og tilganger kan gis. Databehandleravtalen varierer med bruksområde fra det enkle med referanse til personopplysningslovens krav, til mer detaljerte sikkerhetskrav i egne sikker-hetsbilag. Når det kommer til driftsfasen, er det databehandleravtaler som regulerer tilgang til pasientinformasjon. Som eksempel nevnes at pasient-informasjon ikke skal hentes ut uten at databehandlingsansvarlig er informert og har akseptert dette. Tilgang skal varsles og godkjennes. Noen aktører oppgir at det kan være en utfordring i kontrollspennet når leverandørene har mange underleverandører i flere land.

6.1.5 Velferdsteknologi med nye leveranseformer

Noen aktører og leverandører nevner at det innenfor e-helsetjenester, og ikke minst velferdsteknologi, skjer en utvikling der private leverandører i et internasjonalt marked i økende grad tilbyr tjenester de selv driver. Medisinsk-teknisk utstyr kan kobles opp mot smarttelefoner og overføre data til journalen. Et eksempel er blodsukkermålere og insulinpumper for personer med diabetes. Stadig flere enheter som er koplet til internett (som biologiske sensorer m.m.), maskinlæring og kunstig intelligens blir i økende grad mer tilgjengelig i pasient-nære mobile applikasjoner og plattformer. Private leverandører tilbyr allerede en rekke slike løsninger til privatpersoner. Det etterlyses derfor tydelige retnings-linjer rundt pasientnære løsninger med innslag av skyløsninger. Det er for eksempel behov for avklaring av ansvarsforhold der noen leverandører ønsker full tilgang til data i behandlingshjelpemidler. Utviklingen innebærer at virksom-hetene må forholde seg til løsninger som er kjøpt av privatpersoner eller organisasjoner, og ikke er anskaffet gjennom virksomhetene.

Den tradisjonelle delingen mellom basisdrift og applikasjonsdrift vil endres gjennom denne utviklingen, og leverandørene vil få en større rolle innenfor for eksempel sikkerhetsovervåkning. For pasientrettede systemer vil det i mange tilfeller være tjenester som ligger tett opp til det som sektoren anser som sine kjerneoppgaver. Denne utviklingen vil stille nye krav til risikovurdering og kontroll med pasientinformasjon.

6.2 Forslag til kriterier, rutiner og tiltak knyttet til forbedringsområder

De viktigste kriterier og rutiner for å kunne håndtere og ivareta informasjonssikkerhet og personvern ved bruk av private leverandører er:

- **God og reell ledelsesforankring og styring**
  Virksomheten må ha en helhetlig styringsmodell med klarhet i ansvar- og roller knyttet til informasjonssikkerhet, som også dekker private leverandører. Et kompliserende forhold hos helseforetak / regionale helseforetak er strukturen der databehandlingsansvaret ligger plassert hos hvert enkelt helseforetak, og kompleksiteten dette skaper i sikkerhetsstyring av regionale og nasjonale tiltak.

- **Helhetlig risikovurdering**
  Når tjenester overlates til private leverandører må det foretas en helhetlig risikovurdering slik at den totale risikoen kommer frem og rapporteres til ledelsen. Risikovurdering og tiltak må ta høyde for de begrensinger som finnes i nåværende eldre og komplekse tekniske løsninger.

- **Behov for kompetanse**
  Virksomheten må ha tilgjengelig og tilstrekkelig kompetanse for å ivareta sitt ansvar for informasjonssikkerhet og personvern når private leverandører benyttes. Bestillerkompetansen må være god nok til å følge opp leveranser i alle faser fra kravstilling til leverandøroppfølging i en driftsfase. For spesialisthelsetjenesten vil en del av denne kompetansen finnes blant annet i regionale IKT-enheter og Sykehusinnkjøp. Ledelsen, inkludert styret, må ha tilstrekkelig kompetanse for å utøve reell styring og kontroll også på dette området. Helse- og omsorgssektoren kan ha mye å lære av andre sektorer med lengre erfaring med utkontraktering, som for eksempel finanssektoren.

I dette kapittelet presenteres kriterier og rutiner knyttet til informasjonssikkerhet som den enkelte virksomhet selv må vurdere å iverksette. Begrepet rutiner benyttes i denne rapporten generisk og omfatter også prosesser, policy og områder som det bør finnes prosedyrer på. Innholdet er overordnet og beskriver kjernen i det virksomhetene selv kan utdype i mer detaljer. En del av kriteriene og rutinene kan også være et godt grunnlag for mer utdypende veiledningsmateriale som utarbeides gjennom utvikling av Normen. Kriteriene er oppsummert i vedlegg 10.

Kriterier, rutiner og forbedringsområder er nedenfor gruppert på følgende måte:

- Ledelse og forankring
- Risikostyring
- Tre faser av relasjonen til leverandøren
  - Planlegge, vurdere og velge leverandør
  - Inngå kontrakt og oppstart med leverandør
  - Oppfølging og rapportering

Denne modellen viser relasjonen mellom områdene:

Innenfor hver av disse områdene er det gjort:

- Kort oppsummering av utfordringsbildet og begrunnelse for kriterier og rutiner.
- Kriterier
- Rutiner

6.2.1 Ledelse og forankring

Det er et ledelsesansvar å sikre at virksomheten følger krav til informasjonssikkerhet og personvern. Dette omfatter blant annet å håndtere risiko på en helhetlig måte og sørge for velfungerende styring og kontroll.[26] I de tilfellene det skjer svikt på området, kan ofte en medvirkende årsak være at informasjonssikkerhet og personvern håndteres på et for lavt nivå i organisasjonen, uten at ledelsen er reelt engasjert og informert. Informasjonssikkerhet og personvern oppfattes ofte som et vanskelig fagområde i grenselandet mellom teknologi og juss. Ledelsen må sørge for at

26 Se for øvrig til «Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten» som trådte i kraft 1.1.2017.

informasjonssikkerhet vurderes og behandles i et virksomhetsperspektiv. Ledelsen må også holde seg oppdatert på betydning av økende digitalisering og endret trusselbilde, samt nye leveransemodeller for IKT-løsninger. Dette kan for eksempel være skyløsninger.

Håndtering av informasjonssikkerhet og personvern ved bruk av private leverandører må være en del av virksomhetens daglige aktivitet. Virksomhetens styringssystem for informasjonssikkerhet ISMS (Information Security Management System) må være grunnlag for dette arbeidet. Under arbeidet med rapporten har Direktoratet for e-helse fått innspill fra representanter for flere sektorer om at ledelsesforankring er en forutsetning for å lykkes på området, og at vellykket styring og kontroll krever at det er sammenheng i blant annet kravstillelse, risikohåndtering og kommunikasjon helt fra styret til ytterste ledd i underleverandørkjeden. På dette området kan helse- og omsorgssektoren ha noe å lære av bransjer som har mer erfaring med disse problemstillingene. I IKT-forskriften[27] stilles det for eksempel krav til at avtaler om utkontraktering av IKT-virksomhet, og endringer i slike avtaler, skal behandles av styret. Styret skal forelegges planer for utkontrakteringen, med risikovurdering, og en beskrivelse av hvordan foretaket skal sikre leveransen. En tilsvarende ordning kunne med fordel vært implementert hos helsevirksomheter som har et styre (Ref. helse-foretaksloven § 28). Direktoratet for e-helse foreslår at dette implementeres som rutiner i virksomheten (se under), men en kunne også tenke seg at relevante deler av IKT-forskriftens krav til utkontraktering speiles i Normen som krav til sektoren.

Involvering av organisasjonen (stakeholder management) er også et suksess-kriterium. Både for å bygge sikkerhetskultur, men også for å forberede organisasjonen på eventuelle nye arbeidsformer eller rutiner som følge av nye tjenester levert av private leverandører. God involvering av hele organisasjonen vil også legge til rette for informasjonsflyt og åpenhet. Dette vil igjen kunne bidra til at informasjon om for eksempel trusler flyter uhindret opp til toppledelse og styret.

27 Se dokumentoversikt i kapittel 7.

Kriterier:

- Virksomheten må ha en helhetlig styringsmodell med klarhet i ansvar og roller knyttet til informasjonssikkerhet som også dekker bruk av private leverandører.
  - Styringsmodellen må ta høyde for nye behov og krav som oppstår ved bruk av private leverandører.
  - Styringsmodellen må dekke leverandørstyring fra anskaffelse til avtalen er avsluttet. Ved bruk av store og internasjonale leverandører stiller dette andre krav til leverandørstyring. Disse har også sine egne styringsmodeller som man må forholde seg til og som må kontraktfestes.
- Virksomhetens styre og ledelse skal jevnlig oppdateres på status for informasjonssikkerhet og personvern.
- Som hovedregel bør styret og ledelse involveres i tilfeller som gjelder bruk av private leverandører og/eller utkontraktering av et visst omfang.

Rutiner:

- Det må finnes rutiner for hvordan rapportering på saker som gjelder informasjonssikkerhet og personvern skal være tilpasset de ulike nivåene i organisasjonen, inkludert involvering av styret og ledelse.
  - Rapportering må inngå som del av en helhetlig styringsmodell i virksomheten.
  - Rapportering må sikre at risikobildet rundt leveranser fra private leverandører fremkommer på en riktig og forståelig måte.
  - Det bør finnes rutiner for hvordan styre og ledelse planmessig skal kunne holde seg oppdatert på utviklingstrekk innenfor informasjonssikkerhet og personvern.

I arbeidet med rapporten er det på dette området funnet noen forbedringsområder knyttet til komplekse styringsmodeller og kompetanse. Se kapittel 6.3.

6.2.2 Risikostyring

Virksomheten har ansvar for risikostyring og internkontroll også der deler av virksomheten er utkontraktert til private leverandører. Risikostyring må omfatte alle faser fra sourcingstrategi og anskaffelse til avtalen er avsluttet.

Gode og komplette risikovurderinger er svært viktig i arbeidet med informasjonssikkerhet. De er en nødvendig del av rutinene ved anskaffelse, implementering og kontroll. Resultatene fra risikovurderingene inngår som kriterier for beslutninger, samt som grunnlag for å iverksette risikoreduserende tiltak. Ved utkontraktering er det god praksis at risikovurderinger gjøres tidlig, gjerne allerede som en del av sourcingstrategien. Risikovurderingen bør holdes opp mot virksomhetens potensielle gevinster og skadevirkninger må vurderes for virksomheten som helhet.

Vi beskriver her nærmere risikostyring for å sikre informasjonssikkerhet ved bruk av private leverandører i følgende faser:

- Oppstart av risikovurdering
- Gjennomføring av risikovurdering
- Oppfølging og rapportering

I denne rapporten beskrives ikke en komplett metodikk for risikostyring eller risikovurdering, men en del kritiske suksessfaktorer i arbeidet med risiko-vurdering i forbindelse med håndtering av informasjonssikkerhet ved bruk av private leverandører.

Videre er det identifisert ett område der det er spesielt krevende å håndtere risiko. Dette gjelder velferdsteknologi som privatpersoner tar i bruk, og er omtalt som eget forbedringsområde.

6.2.2.1 Oppstart av risikovurderingen

Risikovurdering må skje tidlig i enhver prosess, og må også være gjenstand for revidering og oppdatering for å ta hensyn til blant annet endringer i trussel-bildet, leverandørstrukturer og leveranse. De som utfører risikovurderingene må ha riktig kompetanseprofil og en tydelig eskaleringsvei til ledelsen og styret.

Risikovurderingens omfang eller mandat er viktig. Særlig i risikovurderinger av større løsninger kan det, i tillegg til å se på trusler mot konfidensialitet, integritet og tilgjengelighet, være relevant å ha et litt bredere perspektiv. Dette kan inkludere å vurdere hendelser ut fra nasjonal betydning for helse- og omsorgstjenesten totalt. For å avdekke om dette er relevant kan risikovurderingen innledes med en verdivurdering.

Utfordringer ved risikovurderinger:

- Små tekniske detaljer overskygger store risikoer som oversees eller ikke kommer frem.
- Risikovurderingen gjøres for sent i anskaffelsesprosessen, f.eks. først når løsningen skal settes i drift.
- Risikovurderingen gjøres ut fra en sjekkliste med ja- eller nei-svar uten å ta stilling til hvilke verdier man skal beskytte, og hvilke sårbarheter man vil redusere.
- Risikovurderingene gjøres kun ut fra et IKT-perspektiv.
- Risikovurderingen gjøres kun ut fra regulatoriske krav.
- Risikovurderingen gjøres kun som en vurdering av endring i risiko.
- Uklar eller ulik forståelse av risikobegreper og for eksempel at risikonivåer brukt i risikomatriser ikke tilsvarer de samme som benyttes i virksomhetens styringssystem.

Av svarene fra aktørene i helse- og omsorgssektoren fremgår det at risikovurderinger gjøres i stort omfang, men som Pasientreiser bemerker: «Disse (risikovurderingene) synes likevel ikke dekkende for de faktiske forholdene, siden de fleste beslutningene som er relevante for vurderingene er tatt før risikovurderingene utarbeides.» PwC-rapporten påpeker en rekke forhold rundt risikovurderinger, som at «Sentrale informasjonssikkerhetsrisikoer knyttet til ESN-kontrakten har ikke blitt tilstrekkelig vurdert» og at risikovurderingene er gjort primært i forhold til endringene i risikobildet ved bruk at privat leverandør. Flere peker på at risikovurderinger ikke må gjøres for sent i prosessen og ikke rett før en tjeneste skal settes i produksjon.

Risikovurdering bør gjennomføres for både total risiko for området hvor det skal kjøpes tjenester fra privat leverandør, og ved endret risikobilde knyttet til tjenestekjøp fra den valgte private leverandøren.

En forutsetning for å gjøre en tilstrekkelig risikovurdering er at man har god oversikt over nåværende IKT-infrastruktur og IKT-løsninger i virksomheten, herunder en gradering av personopplysninger fra sensitive til ikke-sensitive. Man må ha oversikt over gjensidige avhengigheter utenfor og innenfor virksomheten. Dersom man ikke har denne oversikten over hele verdikjeden, kan det være en utfordring å vurdere risikobildet.

6.2.2.2 Gjennomføring av risikovurdering – hvilke risikomomenter bør tas med i vurderingen

Risikovurderingen skal dekke det totale risikobilde og endringer i risikobilde gitt leveranser fra private leverandører. Det må angis tydelig hva risikoene er og hvilke risikoreduserende tiltak som må gjennomføres for å få risiko ned på et akseptabelt nivå. Dette kan være tekniske og organisatoriske tiltak som er mulige å gjennomføre innenfor rammen av leveransen. Selv om flere virksomheter i sektoren har gamle eller komplekse løsninger, kan visse tekniske tiltak ofte gjennomføres for å forbedre sikkerheten. For eksempel opprette mer finmaskede tilganger i verktøy for identitet- og tilgangsstyring, automatisk håndheve tilgangsregler og logge alt som gjøres når personell er pålogget kontoer med vide tilganger. Dersom tekniske tiltak ikke er tilstrekkelig for å redusere risiko til et akseptabelt nivå, må dette kompenseres med andre tiltak som strengere fysisk overvåking, etterkontroll og grundigere bakgrunnssjekker.

Risikovurdering, som nevnt ovenfor, må avgjøre i hvilken grad det må gjøres oppgraderinger i sikkerhetsløsninger før den private leverandøren kan gis nødvendig tilgang. Dette kan medføre at deler av kontrakten kan gjennomføres, mens andre deler må vente til tiltak er på plass. Det er viktig at det lages realistiske planer for prosjektgjennomføringen slik at nødvendige sikkerhetsmekanismer kommer på plass.

I tråd med kravene i GDPR skal det gjennomføres en personvernkonsekvens-vurdering (DPIA) dersom behandlingen av personopplysninger «vil medføre en høy risiko for fysiske personers rettigheter og friheter». Det kan være hensiktsmessig å gjennomføre en slik vurdering samtidig med risikovurdering av løsningen.

Momenter som bør besvares av risikovurderingen

- Vil leverandøren kunne få tilgang til pasientinformasjon?
  - Hvilken type pasientinformasjon gjelder det (sensitive/ikke-sensitive opplysninger)
  - Omfang på tilgang og i hvilke situasjoner?
  - Hvordan begrense tilgang til kun de områder som er nødvendig og for angitt formål og tidsperiode?
- Hvordan er tilgangsstyringen sikret for tidsperioden hvor tilgang må gis?
- Hvordan er pasientinformasjon sikret (For eksempel kryptering og signering, anonymisering, aggregering og pseudonymisering)?
- Hvordan kan man spore hva leverandøren har utført og hatt tilgang til? Hvordan oppdage eventuelle avvik (For eksempel logging av tilganger til tekniske løsninger, dataelementer og verktøystøtte for håndtering av hendelser og endringer, samt konfigurasjonsstyring)?
- Hvor gode er leverandørens interne kontrollrutiner?
- Hvor komplekst er aktørbildet (løsninger, produkter, aktører, under-leverandører, verdikjeder)?
- Jurisdiksjon – hvilke land befinner personer i, som kan komme til å få tilgang til pasientinformasjon eller hvor lagres disse data?
- Hvordan håndteres driftsavbrudd og kriseberedskap? (Spesielt relevante tema dersom leverandøren har ansvaret for en tjeneste av viss kritikalitet)

Ved landrisikovurdering mener Finanstilsynet at vurderingene må gå helt ned på det konkrete miljøet og den kulturen som gjelder hos tjenesteyter, og det kan være lav risiko i avgrensede profesjonelle høykompetente miljøer i et antatt høyrisiko land, og høy risiko i et lokalt forretningsmiljø innen det som generelt ansees som et land med lav risiko.

Eksempel fra Finanstilsynet for kriterier knyttet til vurdering av land:

- Finansiell stabilitet
- Politisk stabilitet
- Levestandard
- Teknisk infrastruktur
- Tilgang på kompetanse – utdanningssystem
- Reguleringer – lover – regler – politi – rettsvesen
- Relevante hendelser i landet

6.2.2.3 Oppfølging og rapportering

Når risikovurderingen er avsluttet, vil leveransen være en rapport som viser hvordan risiko er håndtert, og anbefalinger til tiltak. Det er viktig at dette kommuniseres opp til riktig beslutningstakernivå i virksomheten, og på riktig detaljnivå. I denne rapporten understrekes betydningen av styrets involvering for å sikre fokus på sikkerhetsarbeidet. Dette gjelder ikke bare for det enkelte prosjekt eller den enkelte anskaffelse, men som en integrert del av virksomhetsoppfølging.

For å sikre god oppfølging, er det viktig at det skjer en formell godkjenning av plan for risikohåndteringsplan/risikoaksept og oppfølging av tiltak. Godkjenningen må være gjort på ledelsesnivå i tråd med gjeldende fullmaktsmatrise.

For å oppnå effektiv kommunikasjon av risikoer til ledelse og styret kan det være effektivt å bruke like begreper og klare definisjoner på tvers av virksomheten, og også gjerne for sektoren. Videre kan et suksesskriterium være at IKT risiko-begrepene er tilpasset samme terminologi som for annet risikoarbeid i virksomheten (Dette ble påpekt fra en stor aktør i en annen sektor som viktig for god sikkerhetsrapportering).

Oppsummering av kriterier og rutiner for risikostyring:

Kriterier:

- Risikostyring må omfatte alle faser fra anskaffelse til avtalen er avsluttet, og må startes på et tidlig stadium. Risikovurderinger må revideres og oppdateres ved endringer.
- De som utfører risikovurderingene må ha riktig kompetanseprofil og ha en tydelig eskaleringsvei til ledelsen/styret.
- Risikovurderingen har et mandat/omfang som er dekkende nok
- Virksomheten har oversikt og dokumentasjon på hvordan de ulike komponentene som inngår i verdikjeden henger sammen – fra egen infrastruktur til underleverandører. Man må forstå hvilke deler som vil berøres av de tjenestene som den private leverandøren skal utføre.
- Etter at risikovurderingen er foretatt, foreligger det en formelt godkjent plan for risikohåndtering/risikoaksept og oppfølging av tiltak.
- Resultater fra risikovurderingen, risikohåndteringsplan og plan for oppfølging av tiltak er kommunisert på rett detaljnivå til overordnet ledelse og styret.

Rutiner:

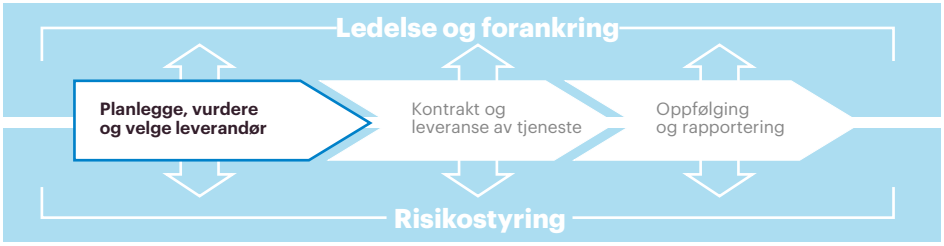
- Det skal finnes rutiner som sikrer at kriteriene beskrevet ovenfor kan oppfylles. Dette bør innarbeides i virksomhetenes eksiterende metodikk for risikovurderinger og risikostyring.

6.2.3 Planlegging, leveranser, og oppfølging

Det er vesentlig at sikkerhetshensyn ivaretas i alle faser av relasjonen til leverandøren med underleverandører, fra planlegging av en anskaffelse til avslutning av kontrakten. Dette krever god bestillerkompetanse i virksomhetene.

Kriterier og rutiner er knyttet til tre generiske faser i leverandørrelasjonen. Modellen angir ikke konkret fasene i et prosjekt, for eksempel anskaffelse og gjennomføring.

6.2.3 .1 Planlegge, vurdere og velge leverandør



Denne fasen omfatter planlegging og gjennomføring av en anskaffelse.

Det er viktig at virksomheten i denne fasen tar stilling til hvilke sikkerhetskrav som skal stilles i anskaffelsen. Enkelte anskaffelsesformer kan være utfordrende med tanke på sikkerhet, fordi kravene til sikkerhet ikke er spesifisert tidlig nok i prosessen og i noen tilfeller ikke ferdig spesifisert før inngåelse av kontrakt. Uansett bør sikkerhet være en del av arbeidet med IT-strategi/sourcingstrategi og gi overordnede føringer.

Både de som tar beslutninger om anskaffelsene og de som leder prosessen må ha den nødvendige bestillerkompetanse tilgjengelig. Bestillerkompetanse innebærer blant annet kompetanse innen:

- Behovet som anskaffelsen skal dekke
- Juridiske rammer, herunder anskaffelse og avtaler, personvern og informasjonssikkerhet
- IKT, inkludert sikkerhetskompetanse
- Prosjektgjennomføringskompetanse
- Leverandørstyring

En del krav vil være gitt på forhånd, for eksempel gjennom eksisterende avtalemessige forpliktelser. Normen er et eksempel på dette. Imidlertid oppleves Normen som for vanskelig av en del virksomheter, samtidig som særlig større virksomheter peker på at den ikke er dekkende nok. Dette er omtalt spesielt i kapittel 6.3.7. Noen leverandører oppfatter enkelte sikkerhetskrav som «særnorske» og dermed vanskelig å implementere, fordi leverandørindustrien til dels er internasjonal. Dette er drøftet i kapittel 6.3.6. Videre kan det være prosjekter som er av en slik karakter at sikkerhetslovens bestemmelser om varslingsplikt ved anskaffelse til kritisk infrastruktur kan komme til anvendelse. Dette er omtalt i kapittel 6.3.4.

Kriterier:

- Virksomhetens styringssystem for informasjonssikkerhet skal inneholde rutiner for håndtering av leverandører. Rutinene skal være integrert med virksomhetens anskaffelsesprosesser.
- Det skal sikres at relevante sikkerhetskrav inngår i alle anskaffelser, og at nødvendig kompetanse på sikkerhet og personvern medvirker i kravstilling og evaluering.
- Tilstrekkelig bestillerkompetanse på alle nødvendige områder.

Rutiner:

- Beskrive hvordan nødvendig bestillerkompetanse er sikret i anskaffelsesprosjekter, herunder kompetanse på sikkerhet og personvern skal inngå i anskaffelsesprosjektet i forbindelse med kravstilling, evaluering og eventuelt forhandling.
- Klassifisere informasjon som vil bli delt med leverandør
  - Det er ikke alltid opplagt om informasjon er sensitiv eller ikke. Et eksempel er fakturavedlegg som kan inneholde helseopplysninger.
- Identifisere relevante sikkerhetskrav for eksempel på bakgrunn av risikovurderinger, regulatoriske krav og krav som følger av avtaleforpliktelser. Det må bestemmes hvordan disse skal vektes, og om enkelte sikkerhetskrav skal være obligatoriske.

6.2.3.2 Inngå kontrakt, oppstart med leverandør

Denne fasen omfatter etablering av kontrakt, og prosessen fram til driftsfase, for eksempel der en fjernaksessløsning er etablert, eller en tjeneste er i produksjon. Her vil det være viktig at nødvendige sikkerhetskrav, for eksempel retten til revisjon er tatt inn i kontrakten. En implementeringsfase eller transisjonsfase vil ofte være preget av aktiviteter knyttet til testing, dokumentasjon og etter-prøving av at tjenester og løsninger oppfyller krav, blant annet sikkerhetskrav. Det kan være aktuelt å ta stilling til i hvilke situasjoner test skal skje på reelle produksjonsdata. En erfaring fra Helse Sør-Øst saken er at leverandøren måtte få tilgang til eksisterende infrastruktur i en mellomfase som var mangelfullt risikovurdert og hvor sikkerhetsmekanismene ikke var på plass.

Tilgangsstyring og kontroll

Implementering av tiltak vil ofte bli komplisert fordi porteføljen av applikasjoner og teknisk plattform i helse- og omsorgssektoren er omfattende, av eldre dato og flere steder fragmentert. Flere av dagens løsninger understøtter ikke alle de sikkerhets-mekanismer som er relevante for å skjerme pasientinformasjon. Implementering av sikkerhetsmekanismer må uansett vurderes opp mot dekning av funksjonelle krav.

Mekanismer for tilgangsstyring i applikasjoner er til en viss grad på plass i kliniske systemer i dag. Disse mekanismene er ikke alltid tilstrekkelig for å sikre pasient-informasjon for flere av de tjenestene private leverandører bistår med. For eksempel kan ansatte hos private leverandører få administratorrettigheter til infrastruktur og systemer, og kan med dette ha «direkte» tilgang til pasientinformasjon.

Eksempler på tekniske tiltak for styring og kontroll av IKT-personells tilgang til pasientinformasjon:

- Identitet- og tilgangsstyring for privilegerte brukere
- Sporing
- Sikre forbindelser og arbeidsflater
- Kryptering og signering
- Anonymisering, aggregering og pseudonymisering
- Automatisk deteksjon av sårbarheter og mulige angrep
- Verktøystøtte for håndtering av hendelser og endringer, samt konfigurasjonsstyring[28]

28 Se vedlegg 5 for nærmere beskrivelse av disse mulighetene.

I PwCs rapport fra ekstern gjennomgang av programmet for modernisering av IKT-infrastruktur (iMod) i Helse Sør-Øst, var identitet- og tilgangsstyring og sporing blant de identifiserte utfordringer og mangler. Planen var at bedre sikkerhetsmekanismer skulle komme på plass i en etterfølgende fase.

Komplekse leveransemodeller

Leveransemodellene til flere IKT-leverandører blir mer komplekse fordi de i stor grad bruker leveransesentre flere steder i verden. Dette inkluderer også norske leverandører. Noen leverandører anvender «følg-solen»-prinsippet, det vil si overvåking flyttes fra land til land gjennom døgnet. I tillegg vil komplekse eierstrukturer og bruk av underleverandører føre til utfordringer med å ha full kontroll med verdikjeden og sikre at det er databehandleravtaler med alle parter. Manglende kontroll rundt dette ble påpekt i PwC-rapporten hvor Hewlett-Packard Norge AS/Enterprise Services Norge AS så langt ikke har kunnet dokumentere at det foreligger databehandleravtaler med samtlige under-leverandører som oppfyller kravene i avtalen med Sykehuspartner.

Det skjer også løpende endringer i eierstruktur slik at det kreves en kontinuerlig oppfølging av leverandørene.

I disse komplekse strukturene er vurderinger av land en viktig faktor. Det er fra flere reist spørsmål om det er enkelte landområder, land eller områder innen et land, hvor det frarådes å sette ut tjenester til. En liste over hvor det generelt er trygt og ikke er trygt å få levert tjenester fra, er nevnt som ønskelig. Både enkelte leverandører og noen tjenestekjøpere har gjort slike vurderinger, se vedlegg 8. Etablering av en eventuell felles veiledende liste bør bygges på råd fra Nasjonal sikkerhetsmyndighet og lages på tvers av sektorene og med et sentralt oppdateringsansvar. Normen kan for eksempel vise til metodikk og bakgrunnsinformasjon for landrisikovurderinger hos andre myndigheter som Nasjonal sikkerhetsmyndighet. Det understrekes at dette ikke fritar virksomheten fra vurderingsansvar.

Ved vurdering av risiko ved foreslått leverandørstruktur bør det det også kreves beskrivelse av, og eventuelt innsyn i, de interne rutiner og mekanismer som leverandøren har og hvilke sertifiseringer leverandøren har.

Kriterier:

- Det er kvalitetssikret at kontrakten inneholder nødvendige sikkerhetskrav.
- Det er definert hva slags sikkerhetstesting som skal foretas, for eksempel penetrasjonstest for å verifisere at kundens data er sikre.
- Det er etablert tydelige, omforente planer for etablering av sikkerhetstiltak på bakgrunn av risikovurderinger som er gjort. Inkludert, dersom tekniske tiltak ikke er gode nok, hvilke andre tiltak er innført for å få akseptabelt risikonivå.
- Rutinene i Normens fjernaksessveileder følges.

Rutiner:

- Etablering av databehandleravtale i de tilfellene dette er relevant (leverandøren behandler data på vegne av den databehandlingsansvarlige)
- Databehandlingsansvarlig skal på forhånd godkjenne databehandlers eventuelle underleverandører
- Rutiner / standardiserte kontraktsvilkår:
  - Behovet for at leverandørens underleverandør oppfyller de samme sikkerhetskravene som stilles til leverandøren.
  - Krav om rapportering og håndtering av sikkerhetshendelser.
  - Retten til å utføre testing og revisjon hos den private leverandøren og dens underleverandører. Frekvens, type revisjon, og ev. bruk av 3. partsrevisjon bør angis.
  - Behovet for sikkerhetsrelatert ytelsesovervåkning og rapportering på fastsatte KPI-er (Key Performance Indicator).
  - Muligheten til å reforhandle vilkår og betingelser i kontraktens løpetid (eller ved definerte intervaller) på grunn av endringer i risikonivå.
  - En exitplan og klare vilkår ved avslutning av kontrakten. Dette må omfatte krav om at alle data tilhørende kunden er slettet eller tilbakelevert og rett til en skriftlig erklæring fra leverandøren som bekrefter dette.
- Rutiner for test, blant annet vurdering av i hvilke tilfeller reelle / produksjons data kan benyttes, med tilhørende sikkerhetstiltak. Se for eksempel Normens faktaark om informasjonssikkerhet ved utførelse av testing.[29]
- Leverandørene gir til enhver tid gir en komplett oversikt over hvilke enheter innen strukturen (konsernet og underleverandører) som benyttes for å levere tjenester og i hvilket land disse holder til i, samt at det er inngått databehandleravtaler med alle aktører.

29 https://ehelse.no/Documents/Normen/Faktaark%2048%20-%20Informasjonssikkerhet%20ved%20utf%C3%B8relse%20av%20testing.pdf

6.2.3.3 Oppfølging og rapportering

I denne fasen vil vesentlige aktiviteter være knyttet til leverandøroppfølging og revisjon. Terminering, fornyelse eller reforhandling av kontrakt omfattes også.

Kriterier:

- Håndtering av løpende landvurderinger / globalt trusselbilde.
- Det gjennomføres jevnlige revisjoner av leverandøren etter en fastsatt plan.
- Løpende oppfølging av at kontraktens krav til sikkerhet og rapportering oppfylles, og at man foretar nye risikovurderinger ved endringer av avtalen.
- Ved terminering av kontrakten skal det etter en fastsatt tid alltid foreligge en signert erklæring fra leverandøren om at alle data tilhørende virksomheten er tilbakelevert eller slettet.
- Om bytte av underleverandør er aktuelt skal virksomheten alltid underrettes og på forhånd godkjenne ny underleverandør.

Rutiner

- Hvordan revisjon av leverandører skal foregå, for eksempel med henvisning til relevante internasjonale standarder.
- Etablering av revisjonsplan.
- Rutiner for løpende oppfølging av kontrakten, inkludert endringer.
- Virksomhetens kontinuitetsplaner bør dekke tilfeller der leverandørens (med underleverandører) tjenester blir utilgjengelige, planlagte eller ikke-planlagt.
- Fremgangsmåte for sletting/tilbakelevering av informasjon ved terminering av kontrakt.

6.3 Beskrivelse av noen konkrete forbedringsområder

Innenfor sikkerhetsområde finnes det flere eksempler på at det er hensiktsmessig å løse utfordringer med felles tiltak, et eksempel er Normen. Et nyere tiltak er HelseID.[30] I denne rapporten presenteres flere forslag som helse- og omsorgssektoren kan løse sammen. Nedenfor følger en nærmere beskrivelse av syv forbedringsområder knyttet til bruk av private leverandører:

- Utforme gode styringsmodeller og tydeliggjøre ansvarsforhold spesielt ved fellesløsninger med flere databehandlingsansvarlige
- Heve kompetanse om IKT-sikkerhet og risikovurderinger
- Tilrettelegge for håndtering av ny teknologi og løsninger tatt i bruk av privatpersoner og som ønskes knyttet til løsninger hvor helsevesenet er databehandler
- Skape klarhet om når sikkerhetsloven kan komme til anvendelse og hvilke konsekvenser det eventuelt får
- Gjøre det enklere å vurdere sikkerhet ved valg av leverandører og løsninger/tjenester
- Særnorske krav rundt behandling av pasientinformasjon – overordnet kartlegging av omfang og forslag til gjennomføring av videre arbeid
- Normen oppleves av noen å være for kompleks for små aktører og ikke heldekkende for de store aktørene

De to første forbedringsområdene relaterer seg primært til ledelse og forankring. Se kapittel 7 for prioritering og nødvendige avklaringer.

6.3.1 Styringsmodell og databehandlingsansvarlig

Utfordring/risikoområde

Det oppleves i sektoren at styringsmodellene er komplekse og uklare hva angår ledelsesansvar og hvilket nivå ansvaret ligger på. Særlig oppleves ansvaret som påhviler databehandlingsansvarlig som uklart. Problemstillingen berøres også av PwC-rapporten, hvor det skrives at: «Systemet for gjennomføring av risiko-vurderinger har ikke fungert som en effektiv kontrollmekanisme. Uklare kriterier for risikoaksept fører til usikkerhet med hensyn til hvem som kan akseptere hvilke risikoer.»

Når for eksempel Sykehuspartner HF, som databehandler for helseforetakene i Helse Sør-Øst, beslutter å inngå et strategisk partnerskap med en privat leverandør om drift, forvaltning og modernisering av regional infrastruktur, er de overordnede mål og strategier som er grunnlaget for beslutningen behandlet og godkjent av styret i det regionale helseforetaket, mens sikkerhetskrav for IKT-virksomheten er helseforetakenes ansvar som databehandlingsansvarlige.

30 HelseID er en felles påloggingsløsning for helse- og omsorgssektoren. Den legger til rette for at helsepersonell kan få engangspålogging (single sign-on) med én elektronisk ID (e-ID) i hele helsetjenesten.

Dersom helseforetakene har ulike sikkerhetskrav er det uklart i hvilken grad det regionale helseforetaket har myndighet til å fastsette felles regionale krav ut fra en helhetlig vurdering.

Fra IKT-leverandørene rapporteres det også at de opplever at ulike aktører i sektoren har ulike risikovurderinger av samme løsning. Leverandører av medisinsk-teknisk utstyr har påpekt at de ofte må gjøre en risikovurdering per installasjon av instrumenter og at vurdering av akseptabel risiko ofte ikke er den samme. Dette kan gjelde også innen samme helseforetak. Det blir også mange databehandleravtaler som må inngås per helseforetak selv om leveransene er basert på en regional anskaffelse.

I spesialisthelsetjenesten kan prinsippet om at et regionalt helseforetak ikke kan være databehandlingsansvarlig for helseopplysninger, bidra til usikkerhet og forskjellige krav og vurderinger. (Jf. forarbeidene til pasientjournalloven Prop. 72 L (2013-2014) kapittel 12.1.2). Særlig utfordrende er fellesløsninger som de regionale helseforetakene anskaffer og etablerer, da disse må risikovurderes av hvert enkelt helseforetak. Det samme gjelder for alle endringer som kan påvirke informasjonssikkerheten i slike fellesløsninger. Dette fører med seg meget komplekse vurderings- og beslutningsprosesser, samt at det kan bli uklart hvem som har ansvaret for den helhetlige risikovurderingen og på hvilket grunnlag det skal vurderes hva som totalt sett er akseptabel risiko.

Problemstillinger om databehandlingsansvar for løsninger som dekker flere virksomheter i sektoren er en utfordring utover spesialisthelsetjenesten, både for primærhelsetjenestene og for nasjonale løsninger. Direktoratet mener det i første omgang bør prioriteres utredning rundt databehandlingsansvar mellom RHF og HF.

Tiltak:

- Det bør utredes om databehandlingsansvaret slik det er i dag er forenlig med strategier for etablering av fellesløsninger i helse- og omsorgssektoren. Det bør særskilt vurderes om det er behov for regulering av felles databehandlingsansvar eller fordeling av dette ansvaret mellom regionale helseforetak og helseforetakene de eier. EUs personvernforordning åpner for å regulere dette i nasjonal rett og arbeidet bør også omfatte eventuelt utkast til regulering.

Forslag til ansvarlig: Direktoratet for e-helse.

Dette bør blant annet baseres på følgende vurderinger:

- EUs nye personvernforordning (GDPR) har en egen bestemmelse om Felles behandlingsansvarlige (Art. 26)[31]. Utgangspunktet er at dersom to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med og midlene for behandlingen, skal de være felles behandlingsansvarlige. De skal fastsette sitt respektive ansvar for å overholde forpliktelsene i forordningen, særlig med hensyn til utøvelse av den registrertes rettigheter og bestemmelsene om informasjonsplikt. Dette gjelder ikke hvis fordelingen av ansvaret er regulert i EU/EØS-retten eller i nasjonal rett. Den registrerte kan i alle tilfeller utøve sine rettigheter overfor hver av de behandlingsansvarlige.
- I høringsnotatet til ny personopplysningslov[32] som gjennomfører personvernforordningen i norsk rett, skriver Justis- og beredskapsdepartementet at det etter gjeldene rett er mulig å dele behandlingsansvaret mellom flere, selv om dagens personopplysningslov og – forskrift ikke har slike bestemmelser. Etter departementets vurdering er det ikke hensiktsmessig å gi generelle bestemmelser om dette, så forslaget til ny personopplysningslov ikke inneholder forslag til nasjonale regler om delt behandlingsansvar. Justis- og beredskapsdepartementet antar at dette trolig best kan reguleres i særlovgivningen, dersom det viser seg å være behov for regler om delt behandlingsansvar på konkrete områder.

Forslaget er at dette i første omgang vurderes for regionale helseforetak og helseforetakene de eier. Resultatet kan eventuelt også få anvendelse for primærhelsetjenesten og sentrale løsninger.

31 https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/uoffisiell-norsk-oversettelse-av-personvernforordningen.pdf

32 https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/horingsnotat--ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett.pdf

6.3.2 Kompetanseheving på informasjonssikkerhet

Utfordring/risikoområde

Informasjonssikkerhet blir stadig viktigere for sektoren og området blir mer komplekst. Dette krever økt kompetanse, ikke minst på ledelse- og styrenivå. Dette gjelder både for å kunne se på risiko i et helhetlig perspektiv og konkret kompetanse innen IKT-sikkerhet. Uten tilstrekkelig kompetanse på dette området, er det vanskelig for ledelsen fullt ut å forstå de risikobedømminger som gjøres og ta de riktige beslutningene. Svak kvalitet på risikovurderinger tas opp som utfordring fra flere.

For å oppnå god styring av de private leverandørene, må foretakene i større grad enn i dag bygge opp en kompetent sikkerhetskultur, ikke minst på ledelsesnivå.

Kriterier:

- Tydelige krav til nødvendig kompetanse innen informasjonssikkerhet og risikovurderinger hos blant annet:
- Ledelsen og styret
- De som arbeider med anskaffelsene (bestillerkompetanse)
- De som arbeider med innføring og oppfølging

Rutiner:

Eksempel på rutiner som er viktige ved kjøp fra private leverandører i et større marked:

- Rutine som sikrer at det er tilstrekkelig basiskompetanse i styre og ledelse, inkludert forståelse av forhold som kan påvirke informasjonssikkerhet og tilgang til pasientinformasjon.
- Rutiner som sikrer at det er tilstrekkelig bestillerkompetanse i alle enheter som deltar i anskaffelser og leverandøroppfølging.
- Rutiner for kompetansehevende tiltak for å møte endringer som påvirker informasjonssikkerhet og risikobildet i leveransene.

Tiltak:

- Etablere forum for deling av beste praksis og erfaringer i sektoren på områder som sikkerhetskultur og kompetanseutvikling. Det er naturlig at dette sees i sammenheng med oppdraget om kompetanseutvikling innen informasjonssikkerhet som Direktoratet for e-helse har i samarbeid med Norsk Helsenett.
- Sektorens bør utvikle felles opplegg/plan for å sikre at opplæringstilbud til ledere og ansvarlige beslutningstakere innen sikkerhetskompetanse er på et tilstrekkelig nivå.

6.3.3 Håndtering av ny teknologi og løsninger tatt i bruk av privatpersoner

Utfordring/risikoområde

Utfordringene ved bruk av ny teknologi er mange og kort beskrevet i kapittel 6.1.5, samt i referansematerialet. Hovedaktørene vil måtte legge til rette for at slik teknologi og løsninger skal kunne inngå i helsetjenestetilbudet og helsehjelpen der det er formålstjenlig, samtidig som personvern og sikkerhetskrav må tilfredsstilles.

Arbeider og referanser – velferdsteknologi og medisinsk teknisk utstyr:

Norsk lovgivning på området medisinsk utstyr og håndteringen av utstyret er godt implementert og i tråd med EU- direktivene[33] og Helsedirektoratet er fag- og tilsynsmyndighet[34].

Det er vanskelig å avgrense hva som er «helsehjelp» og hva som er et «konsumentgode» i privatrettslig sammenheng. Krav til sikker håndtering av pasientinformasjon bør være lik for pasientnær e-helse- og velferdsteknologi som det som kreves for lignende løsninger i helsesektor for øvrig. Overordnet er kravene gitt i Normen, gjeldende forbrukerlovgivningen og Datatilsynet har utgitt Veileder Personvern for apputviklere[35].

Velferdsteknologi er i rivende utvikling og stadig flere kommuner er i produksjon, særlig vedrørende trygghetsskapende teknologi i hjemmene.

Tilrettelegging for håndtering av ny teknologi og løsninger tatt i bruk av privatpersoner er også omtalt på Direktoratet for e-helse sitt hjemmeområde[36].

33 Helsedirektoratet – Norsk lovgivning
34 Helsedirektoratet – Klinisk utprøving og evaluering av medisinsk utstyr
35 Datatilsynet – Veileder Personvern for apputviklere
36 Direktoratet for e-helse: Nasjonal referansearkitektur – Velferdsteknologi

Direktoratet for e-helse har i 2016 vurdert om det skal etableres sertifiserings- eller selvdeklareringsordninger på helseapp-området. Det er ikke ønskelig nå på grunn av uavklarte spørsmål i gjeldende lovgivning. Det er derimot et stort ønske om bedre veiledning blant annet fra forbrukermyndighetene, Datatilsynet og direktoratene i helse- og omsorgssektoren.

Problemstillingen antas å være viktig for kommunesektoren, og tiltak bør vurderes for sektoren samlet. Derfor bør en nærmere kartlegging av status og behov i kommunene finne sted først.

Tiltak:

- Det bør tas initiativ for å samordne veiledningen på området, og for øvrig følge med på den nasjonale, nordiske og internasjonale utviklingen på området pasientnære og mobile applikasjoner for helseformål. Forslag til oppfølging er Velferdsteknologiprogrammet.
- Det vises også til ellers til omtale av sertifisering nedenfor. Det må også vurderes om det er behov for å utrede mer om ansvar og sikkerhetsnivå, primært knyttet til databehandleransvar og godkjenninger.

6.3.4 Sikkerhetsloven

Utfordring/risikoområde

Departementet ber i oppdraget om at det sees på forholdet mellom helsetjenesten og sikkerhetsloven. Direktoratet anser at det er spesielt § 29 a i sikkerhetsloven, om nye krav til varslingsplikt ved anskaffelser til kritisk infrastruktur, hvor det fra sektoren etterlyses veiledning.

Paragrafen er ny fra i år (trådte i kraft 1.1.2017) og i tillegg er forslag til ny sikkerhetslov fremmet for Stortinget.

Fra forarbeidene er det særlig to forhold som kan nevnes her. For det første fremgår det at dersom praktiseringen av bestemmelsen blir vanskelig, kan det bli aktuelt å utforme vurderingskriterier i forskrift og at det tas sikte på at det utarbeides veiledningsmateriell til bestemmelsen[37].

For det andre gis det holdepunkter for en ulik tilnærming til kravet for store og mindre virksomheter da det er beskrevet at større virksomheter lettere vil kunne ha tilgang til egne tekniske miljøer og informasjon om trusler enn de mindre. Departementet uttaler også at *«Omfanget av risikovurderingene må tilpasses den enkelte anskaffelse, og virksomhetene har selv ansvaret for å tilpasse ressursbruken.»*[38]

37 Prop. 97 L (2015-2016) side 63–64.
38 Prop. 97 L (2015-2016) side 63.

Det er usikkerhet blant flere aktører i sektoren om sikkerhetsloven får anvendelse på deres aktivitet. Siden konsekvensene er betydelige (anskaffelser kan i ytterste konsekvens stanses), er behovet for veiledning stort.

Det er derfor viktig at det raskt kommer tydelig veiledning fra sentrale myndighetsorganer for § 29 a. Dette inkluderer når og hvordan den kommer til anvendelse.

Se punkt 3.1.5 for videre vurdering av helsetjenesten og sikkerhetsloven.

Tiltak:

Det bør utarbeides veiledningsmateriale til sikkerhetsloven § 29 a. Direktoratet for e-helse kan bistå med kunnskap og vurderinger knyttet til helse- og omsorgssektoren.

Ved større IKT-anskaffelser i sektoren må det vurderes om sikkerhetsloven § 29 a om *«kritisk infrastruktur»* kan være relevant. Ved anskaffelse til noe som kan bli vurdert som *«kritisk infrastruktur»* må risikovurdering etter sikkerhetsloven foretas og overordnet departement varsles dersom det er risiko for at «sikkerhetstruende virksomhet» blir etablert. Direktoratet for e-helse kan bistå departementet med rådgivende uttalelser til departementets videre håndtering av slike saker.

6.3.5 Forenkle vurderingen av sikkerheten ved valg av leverandører

Utfordring/risikoområde

Flere aktører i sektoren mener det er omfattende å vurdere sikkerhet ved valg av leverandører og løsninger/tjenester. Vurderingene tar lang tid, krever mye ressurser og blir likevel ikke så komplette og gode som ønsket. Både forenklinger som ulike godkjenningsordninger, sjekklister, rammeverk og mer kompetansedeling ønskes. Vurderingsarbeidet er sett på som en utfordring for både små og store aktører, for eksempel fastleger, tannleger og RHFene. Noen av innspillene om sertifisering framgår av svarene fra RHFene som er gjengitt i vedlegg 7 «Endringer av krav og rutiner».

IKT-næringen tar også opp dette behovet og støtter forslag til sertifisering/deklarerings-ordninger, primært i henhold til internasjonale normer og standarder.

Det ble i 2012–2013 lagt ned et arbeid med vurdering av en ordning for selv-deklarering for programvare i blant annet Helsedirektoratet i forbindelse med forarbeidet til forskrift om IKT-standarder i helse- og omsorgssektoren. I 2015–2016 sendte Direktoratet for e-helse ut et høringsnotat «Forslag til selv-

deklareringsordning for mobile helseapplikasjoner». Det er ikke planlagt innført noen konkrete ordninger.

Tiltak:

Videre arbeid med eventuelle sertifisering- eller selvdeklareringsordninger bør bygge på det arbeidet som allerede er nedlagt og det som gjøres internasjonalt. Hovedaktørene anbefaler at eventuell sertifisering er et område for EU-harmonisering. Det er kommet innspill om at dette bør bygge på anerkjente globale sertifiseringer/deklareringer innen informasjonssikkerhet for helse- og omsorgssektoren. Problemstillingen er om det skal foretas en ny vurdering og på hvilke områder det gir verdi.

Et annet mulig tiltak er at Normen kan videreutvikles til å inneha en omforent «kravliste» på nasjonalt nivå. Omforente nasjonale krav vil gi sektoren større tyngde i det internasjonale leverandørmarkedet. Denne listen kan baseres på faktaark 6b) med nødvendige tilpasninger og listen kan danne grunnlag blant annet en ISAE3402-attestasjon. Dette er attestasjon som gjør det mulig for en revisor å attestere en tjeneste-leverandørs oppfyllelse av gitte krav. Standarden er mye brukt i andre sektorer og en attestasjonsordning kan være raskere å gjennomføre enn en sertifiseringsordning.

Forslag er at det i første omgang avklares om dette skal vurderes nærmere for sektoren og for hvilke områder det vil gi størst verdi. Dersom tiltaket blir aktuelt, bør det vurderes hvorvidt tiltaket kan underlegges nasjonal styring og samfinansiering blant aktørene i sektoren.

Se også tiltak for kompetanseheving beskrevet i 6.3.2.

6.3.6 Særnorske krav – kartlegging av omfang og videre arbeid

Utfordring/risikoområde

Både fra sektoren og leverandørsiden er det påpekt at opplevelsen av særnorske krav og ulike tolkninger medfører at det brukes ekstra ressurser for å ta i bruk utenlandske løsninger. Direktoratet for e-helse har prøvd å innhente eksempler på særnorske krav, inkludert lovkrav. Det har kommet inn noen eksempler. Disse er primært ulik tolkning av krav og ikke særnorske lovkrav. Men problemet med mange ulike tolkninger skaper også utfordringer for leverandører og kjøpere. Innen rammen av dette oppdraget har det ikke vært mulig å stadfeste omfanget på «særnorske» krav.

Ett RHF skriver: «Det brukes store ressurser for å sikre etterlevelse av krav til informasjonssikkerhet. Ofte krever dette videreutvikling av internasjonale

leverandørers løsninger, dette for å sikre at de tilfredsstiller våre krav. Med innføring av GDPR får vi et felles juridisk rammeverk i EU/EØS, og en harmonisering av praksis innenfor EU og EØS, inkludert Norge, vil gjøre det vesentlig enklere for oss å sikre at de krav som gjelder i Norge (og da også resten av dette området) blir oppfylt. Dette vil ikke bare forenkle anskaffelsene, men også fjerne en betydelig risikofaktor knyttet til innføringen av løsningene, og dessuten legge bedre til rette for bruk av de systemer som vi ser komme innenfor e-helse og velferdsteknologi.»

Ett annet RHF skriver at: «Det er generelt utfordringer knyttet til at leverandør-markedet ikke har tilstrekkelig kjennskap til nasjonale krav. Anbefalingene er at regelverket harmoniseres i større grad internasjonalt, ny EU-forordning er et skritt i denne retningen».

IKT-leverandørene påpeker at særkrav kan medføre at norske virksomheter ikke blir tilbudt de mest moderne og beste tjenester eller løsninger om vi ikke harmoniserer oss med kravene i et globalt marked i fremtiden.

Tiltak:

Særnorske krav og krav som leverandører bare møter i Norge, rundt behandling av pasientinformasjon, bør kartlegges på overordnet nivå for å identifisere omfang. Kartleggingen bør ha fokus på viktige krav basert på innspill fra IKT-leverandørene og et utvalg av de andre aktørene. Basert på dette må det bestemmes eventuelt videre arbeid.

Norske krav bør harmoniseres med krav fra EU og eventuelt internasjonale standarder. Norske myndigheter bør påvirke EU/EØS eventuelt i internasjonale fora slik at «internasjonale krav» innehar tilstrekkelig sikkerhet på nivå med det som er ønsket i Norge.

Tiltak som foreslåes er å utarbeide standardiserte maler for databehandleravtaler.

6.3.7 Normen

Utfordring/risikoområde

Norm for informasjonssikkerhet i helse og omsorgstjenesten, Normen, oppfattes som omfattende og komplisert av mange små virksomheter. Hvis kravene i Normen ikke forstås av virksomhetene som stiller krav til leverandørene, er det tvilsomt om virksomhetene klarer å omsette dette i tydelige krav. Blant de store aktørene er det imidlertid påpekt at Normen bør dekke mer og gi flere føringer og tydelige kriterier.

Helse- og omsorgssektoren består av små og store virksomheter, fra Helse Sør-Øst som er en av Norges største virksomheter med mer enn 70 000 ansatte, til privatpraktiserende leger, psykologer og tannleger. Det er utfordrende å lage felles regler som skal gjelde alle og samtidig være både enkle og dekkende for alle virksomhetene. Utviklingen av Normen, og det meste av øvrig arbeid med informasjonssikkerhet, har primært siktet seg inn mot de store virksomhetene som helseforetakene og de største kommunene.

Men Normen har også veiledningsmateriell for dem som ikke er spesialister på informasjonssikkerhet. Det finnes for eksempel en veileder for legekontor. Denne gir legekontorer et praktisk verktøy i arbeidet med å ivareta gjeldende krav til personvern og informasjonssikkerhet.

Normen videreutvikles i dag etter en plan som innebærer at den over det neste halvåret tilpasses den nye personvernforordningen (GDPR). Denne oppdateringen vil kunne dekke utfordringen med at Normens krav både oppfattes for lite dekkende og samtidig for omfattende. Det vurderes om Normen skal bygges opp på en måte som gjør at vi får færre og lettere forståelige «skal»-krav og flere «bør»-krav. Det kan også være aktuelt at enkelte «bør»-krav blir «skal»-krav dersom de oppfyller gitte kriterier, for eksempel virksomhetens størrelse, type behandling, omfang osv.

Normen er i dag sektorens viktigste virkemiddel for å stille krav til informasjonssikkerhet og personvern. For å operasjonalisere rutinene og kriteriene som beskrives i denne rapporten, vil det være viktig at disse gjenspeiles og detaljeres i Normen. Dette kan skje både gjennom nye bindende krav i Normen, eller som veiledning i faktaark og veiledere. Denne rapporten peker også en del forhold knyttet til komplekse leverandørstrukturer og leveransemodeller. Dette bør også reflekteres i Normen, for eksempel ved å vise til metodikk og bakgrunnsinformasjon for landrisikovurderinger hos andre myndigheter som Nasjonal sikkerhetsmyndighet.

Tiltak:

Vurdere hvordan Normen kan bli et bedre verktøy tilpasset alle brukergruppene.

- Forenkling og eventuell modulisering for å tilpasses ulike brukergrupper
- Struktur og språk (pågår)
- Tilpasset GDPR (pågår)
- Oppdatere Normen slik at den speiler komplekse leverandørstrukturer og leveransemodeller, blant annet gjennom å utdype kriteriene og rutinene omtalt i denne rapporten.

7 Forslag til videre aktiviteter

Dette kapittelet oppsummerer forslag til videre aktiviteter som bør gjennomføres på kort og mellomlang sikt. Forslagene omfatter aktiviteter som vil ha generell betydning i helse- og omsorgssektoren og hvor gjennomføringsansvaret bør legges sentralt. Forslagene er basert på Direktoratet for e-helses funn. I tillegg er det i kapittel 6.2 forslag til flere rutiner og tiltak som den enkelte virksomhet bør iverksette i eget arbeid med informasjonssikkerhet.

I Nasjonal e-helsestrategi 2017–2022 er det et grunnleggende prinsipp at det som kan bli løst nasjonalt, skal bli løst nasjonalt. Å legge til rette for nye samhandlingsformer er viktige tiltak i strategiperioden. Dette omfatter blant annet tilgang mellom virksomheter, grunndataløft, økt sporbarhet, bedre pasientmedvirkning og informasjonsflyt og digital sikkerhetsstrategi for helsesektoren. Disse oppgavene må løses i fellesskap i sektoren. For å få dette til, er det viktig å etablere finansieringsmodeller som gjør det mulig. Direktoratet har anbefalt obligatorisk samfinansiering av viktige nasjonale løsninger.

De anbefalte aktivitetene i dette kapitlet er gruppert som følger:

- Avklaring av databehandlingsansvar mellom RHF og HF
- Oppdatering av Normen
- Kompetanseheving
- Øvrige funn for oppfølging

7.1 Avklaring av databehandlingsansvar mellom RHF og HF

Det legges i dag til grunn at helseforetakene er databehandlingsansvarlige for personopplysninger helseforetaket behandler i sin virksomhet. De regionale helseforetakene har som oppgave å planlegge, organisere, styre og samordne virksomhetene i helseforetakene de eier. RHFene etablerer i stor grad fellesløsninger som helseforetakene benytter til å yte spesialisthelsetjenester og hvor det behandles pasientopplysninger i stort omfang. Som databehandlingsansvarlig må hvert helseforetak risikovurdere løsningene før oppstart og ved alle endringer som kan påvirke informasjonssikkerheten.

- Det bør utredes om databehandlingsansvaret slik det er i dag er forenlig med strategier for etablering av fellesløsninger i helse- og omsorgssektoren. Det bør særskilt vurderes om det er behov for regulering av felles databehandlingsansvar eller fordeling av dette ansvaret mellom regionale helseforetak og helseforetakene de eier. EUs personvernforordning åpner for å regulere dette i nasjonal rett og arbeidet bør også omfatte eventuelt utkast til regulering.

  Forslag til ansvarlig: Direktoratet for e-helse.

Det er viktig å få gjennomført dette arbeidet så raskt som mulig, da dagens kompliserte ansvarsforhold påvirker og forsinker arbeidet med digitalisering i helse- og omsorgssektoren.

7.2 Oppdatering av Normen

Rapporten peker på en del områder hvor Normen kan gi bedre støtte. Det er også kommet opp andre forslag som kan tillegges arbeidet med Normen. Det bør samles og systematiseres «beste praksis» fra blant annet RHFene, med formål å oppnå større harmonisering. Løpende oppdatering av Normen inngår i Nasjonal handlingsplan for e-helse 2017–2022, punkt 1.4.1, Personvern og informasjonssikkerhet, og tiltakene nedenfor må sees som innspill til prioriteringer for det pågående arbeidet.

- Komplekse leverandørstrukturer og leveransemodeller. Bidra til bedre styringsmodeller ved å:
  - Innhente erfaring fra andre sektorer og oppdatere Normen med blant annet sjekklister for attestasjon (se kapittel 6.3.1).
  - Oppdatere rutiner og maler for å understøtte komplekse anskaffelse (se kapittel 6.3.5).
  - Vise til metode og bakgrunnsinformasjon om landrisikovurdering.
- Risikovurdering og – styring. Innhente erfaring fra andre sektorer og aktører i helse- og omsorgssektoren, som innspill til løpende arbeid med Normen (se kapittel 6.3.7). Et mulig tiltak er å speile relevante deler av IKT-forskriftens krav til utkontraktering i Normen.
- Utarbeide standardiserte maler for databehandleravtaler (se kapittel 6.3.6).
- Nasjonal standard for tilgangsstyring - delvurdering som gjelder private leverandører (se kapittel 6.3.6).
- Generell videreutvikling av Normen med forenklinger og tilpassing til GDPR (se kapittel 6.3.7)
- Kriterier og rutiner som omhandles i 6.2 bør vurderes innarbeidet i planen for oppdateringer i Normen.

7.3 Kompetanseheving

Kompetanseheving innen IKT-sikkerhet og risikovurdering på styre og ledelsesnivå må heves (se kapittel 6.3.2.). Det bør vurderes om Norsk Helsenett i samarbeid med Direktoratet for e-helse, som sektorens kompetansesentre for informasjonssikkerhet, kan lede oppgavene med å:

- Etablere et forum for beste praksis i bransjen for kompetanseheving og sikkerhetskultur.
- Utvikle felles plan for å sikre at opplæringstilbud til ledere og ansvarlige beslutningstakere innen sikkerhetskompetanse er på adekvat nivå.

7.4 Øvrige funn for oppfølging

Tiltak som er foreslått:

- Privat velferdsteknologi – Det bør tas initiativ for å samordne veiledningen på området, og for øvrig følge med på den nasjonale, nordiske og internasjonale utviklingen på området pasientnære og mobile applikasjoner for helseformål (se kapittel 6.3.3). Det må også vurderes om det er behov for at det utredes mer om ansvar og sikkerhetsnivå, primært knyttet til databehandleransvar og godkjenninger (se kapittel 6.3.1). Forslag til oppfølging er Velferdsteknologiprogrammet.
- Sertifisering, selvdeklarering og attestasjon av leverandører, løsninger eller MTU – Avklare om dette skal vurderes nærmere for sektoren og for hvilke områder det vil medføre størst verdi (se kapittel 6.3.5).
- Særnorske krav rundt behandling av pasientinformasjon – Overordnet kartlegging av omfang og forslag til gjennomføring av videre arbeid[39] for særnorske krav (se kapittel 6.3.6).
- Sikkerhetsloven og IKT-anskaffelser – Det bør utarbeides veiledningsmateriale til sikkerhetsloven § 29 a. Direktoratet for e-helse kan bistå med kunnskap og vurderinger knyttet til helse- og omsorgssektoren. *Ved større IKT-anskaffelser i sektoren må det vurderes om sikkerhetsloven § 29 a om «kritisk infrastruktur» kan være relevant. Ved anskaffelse til noe som kan bli vurdert som «kritisk infrastruktur» må risikovurdering etter sikkerhetsloven foretas og overordnet departement varsles dersom det er risiko for at «sikkerhetstruende virksomhet» blir etablert. Direktoratet for e-helse kan bistå departementet med rådgivende uttalelser til departementets videre håndtering av slike saker.*
- Kommunesektoren skulle vært inkludert i dette oppdraget, men det har ikke kommet inn tilstrekkelig antall svar for å danne et godt nok grunnlag. Rapporten omhandler derfor ikke kommunesektoren og en egen kartlegging må eventuelt iverksettes som eget oppdrag senere. Utfallet av en slik kartlegging er relevant for blant annet tiltak på området ny teknologi og løsninger tatt i bruk av privatpersoner, og en prioritering bør sees i sammenheng med dette.

39 Ref. NOU 2013:2 Hindre for digital verdiskaping.

8 Dokumentoversikt

I dokumentoversikten gis det henvisning til en del dokumenter som er nevnt i rapporten og noen andre dokumenter som er relevante for problemstillinger knyttet til informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgssektoren. Dokumenthenvisninger og henvisninger til relevant informasjon er også angitt i fotnoter og i vedleggsamlingen.

Rapporter og dokumenter

- **PwC (juni 2017).** *Helse Sør-Øst RHF Rapport fra ekstern gjennomgang av programmet for modernisering av IKT-infrastruktur (iMod).* https://www.helse-sorost.no/Documents/Styret/Styrem%C3%B8ter/2017/20170628/077-2017%20Vedlegg%201%20-%20HS%C3%98%20FY%202017%20-%20Rapport%20iMod%20v%201.0.pdf
- **Direktoratet for samfunnssikkerhet og beredskap (2016).** *Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf
- **Nasjonal sikkerhetsmyndighet (2017).** *Veiledning for sikkerhetsgraderte anskaffelser og anskaffelser til kritisk infrastruktur.* https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-sikkerhetsgraderte-anskaffelser-2017.pdf
- **Nasjonal kommunikasjonsmyndighet (2017).** *EkomROS 2017 – Risikovurdering av ekomsektoren.* https://www.nkom.no/aktuelt/rapporter/_attachment/29084?_ts=15c9b3cff27
- **Nasjonal IKT (2015).** *Strategi for Nasjonal IKT HF – En felles IKT-strategi for spesialisthelsetjenesten 2016-2019* https://nasjonalikt.no/Documents/Saksdokumenter%20for%20styrem%C3%B8te%20og%20PF/Strategi%20NIKT%202016%20-%202019.pdf
- **Helsedirektoratet (2017).** *Overordnede risiko og sårbarhetsvurderinger for helse og omsorgssektoren.* https://helsedirektoratet.no/publikasjoner/overordnede-risiko-og-sarbarhetsvurderinger-for-helse-og-omsorgssektoren
- **Datatilsynet hjemmeside for oppsummering av krav til innhold i databehandleravtaler.** https://www.datatilsynet.no/regelverk-og-skjema/veiledere/hva-betyr/?id=6326

- **Datatilsynet hjemmeside for syv steg til innebygd personvern**
  https://www.datatilsynet.no/regelverk-og-skjema/lage-nye-losninger/innebygd-personvern/
- **Datatilsynets hjemmesider for en mer fullstendig oppsummering og veiledning:**
  https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/overfore/
- **Direktoratet for e-helse: Søk i Normen-dokumenter.**
  https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen

Stortings-/departementsmeldinger

- **Stortingsmelding 9 (2012–2013). Én innbygger – én journal**
  https://www.regjeringen.no/no/dokumenter/meld-st-9-20122013/id708609/
- **Stortingsmelding 38 (2016–2017). IKT-sikkerhet — Et felles ansvar**
  https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/
- **NOU 2015:13 Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden (Lysneutvalget I)**
  https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/
- **Modernisert sikkerhetslov som favner bredere.**
  https://www.regjeringen.no/no/aktuelt/modernisert-sikkerhetslov-som-favner-bredere/id2557584/
- **Uoffisiell norsk oversettelse av personvernforordningen**
  https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/uoffisiell-norsk-oversettelse-av-personvernforordningen.pdf
- **Høringsnotat ny personopplysningslov, gjennomføring av personvern-forordningen i norsk rett**
  https://www.regjeringen.no/contentassets/c907cd2776264a6486b8dd3ee00a4e3d/horingsnotat--ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett.pdf
- **Høyring – ny forskrift om offentlege arkiv**
  https://www.regjeringen.no/no/dokumenter/hoyring--ny-forskrift-om-offentlege-arkiv/id2515364/
- **Høringsnotat. Forslag til selvdeklareringsordning for mobile helseapplikasjoner.**
  http://legeforeningen.no/PageFiles/258283/H%C3%B8ringsnotat-%20Forslag%20selvdeklareringsordning%20mobile%20helseapplikasjoner.pdf

- **Commission decisions on the adequacy of the protection of personal data in third countries** http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Lover og forskrifter

- **Samfunnssikkerhetsinstruksen:**
  https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349
- **Lov om helseforetak m.m. (helseforetaksloven) - LOV-2001-06-15-93.**
  https://lovdata.no/NL/lov/2001-06-15-93
- **Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) - LOV-2014-06-20-42.**
  https://lovdata.no/NL/lov/2014-06-20-42
- **Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) - LOV-2014-06-20-43.**
  https://lovdata.no/NL/lov/2014-06-20-43
- **Forskrift om behandling av personopplysninger (personopplysningsforskriften) - FOR-2000-12-15-1265.**
  https://lovdata.no/SF/forskrift/2000-12-15-1265
- **Lov om behandling av personopplysninger (personopplysningsloven) - LOV-2000-04-14-31.**
  https://lovdata.no/NL/lov/2000-04-14-31
- **Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten - FOR-2016-10-28-1250.**
  https://lovdata.no/SF/forskrift/2016-10-28-1250
- **Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) - LOV-1998-03-20-10.**
  https://lovdata.no/NL/lov/1998-03-20-10
- **Lov om arkiv (arkivlova) - LOV-1992-12-04-126.**
  https://lovdata.no/NL/lov/1992-12-04-126
- **Lov om offentlige anskaffelser (anskaffelsesloven) - LOV-2016-06-17-73.**
  https://lovdata.no/NL/lov/2016-06-17-73
- **Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) - FOR-2003-05-21-630.**
  https://lovdata.no/SF/forskrift/2003-05-21-630
- **Forskrift om objektsikkerhet - FOR-2010-10-22-1362.**
  https://lovdata.no/SF/forskrift/2010-10-22-1362
- **Forskrift om sikkerhetsgraderte anskaffelser - FOR-2001-07-01-753.**
  https://lovdata.no/SF/forskrift/2001-07-01-753

Innhold

VEDLEGG 1: Begrepsforklaringer

Applikasjonsdrift	Tilgjengeliggjøring av programvare for sluttbrukere med tilhørende overvåking, kapasitetsplanlegging, proaktiv drift og patching.
Applikasjonsforvaltning	Applikasjonsforvaltning er funksjonen som administrerer applikasjoner gjennom deres livssyklus. Dette dreier seg for eksempel om vedlikehold i form av feilrettinger og endringer i oppsett for å håndtere endrede behov, samt planlegging, testing og gjennomføring av oppdateringer og mindre oppgraderinger.
Applikasjonsutvikling/-innføring	Applikasjonsutvikling og -innføring dekker utvikling av programvare og å sette opp og integrere nye systemer, eller gjøre omfattende endringer i eksisterende utover vanlig vedlikehold som gjøres som en del av forvaltningen.
Basisdrift	Drift og overvåkning av infrastrukturen, som er nettverk, utstyr, operativsystem, datasenter/datarom, servere, databaser og datalagring, mellomvare, sikkerhetssystemer, lisenser m.m. uten noen form for forretningslogikk.
Databehandlings-ansvarlig	Databehandlingsansvarlig er definert slik i pasientjournalloven § 2: «den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, og den som i eller i medhold av lov er pålagt et databehandlingsansvar» og som sammenfaller med personopplysningslovens definisjon. Dette betyr at den som bestemmer hva personopplysningene skal brukes til og derfor også hvorfor opplysningene samles inn, er behandlingsansvarlig. I praksis vil det være virksomhetens øverste administrative leder som er behandlingsansvarlig. Lederen kan delegere oppgaver nedover i organisasjonen, men den øverste ledelsen har fortsatt ansvaret for at behandling av personopplysninger skjer på en god måte (Datatilsynet).
Databehandleravtale	Forholdet mellom en behandlingsansvarligvirksomhet og databehandleren skal være regulert i en databehandleravtale. Dette reguleres av personopplysningsloven § 13, jf. § 15.
DPIA (Data Protection Impact Assessment)	En konsekvensevaluering, relatert til informasjonssikkerhet, med formål å vurdere hvordan en bestemt handling eller aktivitet påvirker personvernet. Under GDPR er dette noen ganger obligatorisk, som for eksempel ved bruk av personopplysninger til profilering. (https://www.atinternet.com/en/glossary/data-protection-impact-assessment-dpia/; GDPR, artikkel 35, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)
Drift	Summen av alle styrings- og arbeidsprosesser som er nødvendige for å sikre brukerne tilgang til et IKT-system med avtalt kvalitet. Det være seg basis drift- og applikasjonsdrift.

Ekomloven	Lov om elektronisk kommunikasjon. Lovens formål er å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester, gjennom effektiv bruk av samfunnets ressurser ved å legge til rette for bærekraftig konkurranse, samt stimulere til næringsutvikling og innovasjon.
EPJ	Elektronisk pasientjournal, en elektronisk samling av registrerte opplysninger om en pasient i forbindelse med helsehjelp.
Fjernaksess, -styring, -support (eng. remote access)	Med «fjernaksess» menes i dette dokumentet ekstern tilgang fra leverandør til virksomhet via kommunikasjonslinje. Eksempler på anvendelsesområder er feilretting, feilsøking, oppdateringer, fjernadministrasjon, test- og utvikling, overføring av datafiler, driftsovervåking (databaser, servere, lagringsløsninger), behandling av feilmeldinger og datafiler hos leverandør og sending av feildiagnoser, mv. av fagsystemer og IKT-infrastruktur.
Forvaltning	Summen av alle styrings- og arbeidsprosesser som er nødvendige for å opprettholde krav til kvalitet i en IKT-tjeneste (IKT-løsning, metode, prosess etc.) over tid. Forvaltning kan deles inn i Funksjonell forvaltning, Applikasjonsforvaltning og Teknisk forvaltning.
GDPR/PVF	General Data Protection Regulation (GDPR) / Personvernforordningen (PVF) (Forordning 2016/679) er en forordning som skal styrke og harmonisere personvernet ved behandling av personopplysninger i Den europeiske union (EU). Det omhandler også i noen grad behandling som skjer utenfor EU eller overføring av personopplysninger ut av EU. Forordningen trer i kraft 25. mai 2018 og avløser da personverndirektivet (EU-direktiv 95/46/EF).
Helseplattformen	Prosjekt som skal anskaffe og innføre elektronisk pasientjournal for spesialisthelsetjenesten og kommuner i Midt-Norge.
Informasjonssikkerhet	Informasjonssikkerhet handler om å sikre at informasjonen ikke blir kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet eller av uvedkommende (integritet) og er tilgjengelig ved behov (tilgjengelighet) (DIFI). Informasjonssikkerhet er ikke synonymt med data- eller IT-sikkerhet, som heller er subsett av informasjonssikkerhetsbegrepet, og kun omfatter de tekniske aspektene. Informasjonssikkerhet dekker også fysisk og organisatorisk sikkerhet som omfatter lovmessig etterlevelse, styringssystemer, regelverk, prosesser, prosedyrer og avtaler.
Infrastruktur	Infrastruktur er de mest grunnleggende byggesteinene i IKT som datasenter, maskinvare, samband, nettverk og operativsystem. Plattform består også av byggesteiner som kan brukes til å levere applikasjoner. Eksempler er databaser og mellomvare som kjøretidsmiljø og løsninger for integrasjoner, identitet- og tilgangsstyring.
Jurisdiksjon	Domsmyndighet. En domstols myndighet er geografisk, saklig og funksjonelt avgrenset. Det vil si at domstolen bare kan behandle saker som faller innenfor et bestemt geografisk område og som ikke hører inn under en særdomstol.

KIT	Konfidensialitet, integritet og tilgjengelighet. Informasjonssikkerhet handler om å sikre at informasjonen ikke blir kjent for uvedkommende (konfidensialitet), ikke blir endret utilsiktet eller av uvedkommende (integritet) og er tilgjengelig ved behov (tilgjengelighet) (DIFI).
Kritisk infrastruktur	Kritisk infrastruktur er infrastruktur som er kritisk for samfunnet, og som ved en alvorlig svikt medfører at samfunnet ikke vil være i stand til å opprettholde de leveranser av varer og tjenester som befolkningen trenger. I den norske sikkerhetsloven er kritisk infrastruktur definert i § 3 som «anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner». Se også Prop. 97 L (2015-2016) for videre forklaring av begrepet. I sivilbeskyttelsesloven § 3 er legaldefinisjonen «anlegg, systemer eller deler av disse som er nødvendige for å opprettholde sentrale samfunnsfunksjoner, menneskers helse, sikkerhet, trygghet og økonomiske eller sosiale velferd og hvor driftsforstyrrelse eller ødeleggelse av disse vil kunne få betydelige konsekvenser». Se også «Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?» utgitt av Direktoratet for samfunnssikkerhet og beredskap.
Landrisikovurdering	Ved tjenesteutsetting, skal det gjennomføres en landrisiko-vurdering. Med landrisiko forstår vi risikoen for tap som følge av handlinger helt eller delvis under myndighetenes kontroll. Eksempler på landrisiko er nasjonaliseringer, offentligrettslige sanksjoner som for eksempel importrestriksjoner, krig, grense-sperringer eller borgerkrig. Bakenforliggende forhold som ofte fører til økt landrisiko er: • Politisk ustabilitet; korrupte og ukvalifiserte regjeringer, kupp, revolusjoner, anstrengte forhold til nabostater og lignende • Sosial ustabilitet; store sosiale skjevheter, lavt utdanningsnivå, langvarige og ødeleggende streiker med mer • Økonomisk ustabilitet, stort underskudd i handelsbalansen, gjerne i kombinasjon med høy utenlandsgjeld og inflasjon, dårlig infrastruktur (transport og telekommunikasjonsnett), ekstrem avhengighet av enkelte naturressurser etc (Innovasjon Norge)
Lysneutvalget I	Lysneutvalget I kommer med en rekke anbefalinger for å redusere digitale sårbarheter i samfunnet. Denne meldingen gir en oversikt over status på oppfølgingen av utvalgets anbefalinger. Statusoversikten viser at det er behov for å jobbe parallelt med et bredt spekter av områder innenfor IKT-sikkerhet. Vårt samfunn vil aldri kunne være helt beskyttet mot utfall av eller angrep mot digital infrastruktur og digitale systemer, men vi må evne å iverksette de riktige sikkerhetstiltakene for å redusere risikoen og for å kunne gjenopprette normal funksjon så fort som mulig.
Medisinsk-teknisk utstyr (MTU)	Ethvert medisinsk utstyr, inklusiv in vitro-diagnostisk medisinsk utstyr, inkludert programvare og systemløsninger, beregnet for mennesker til diagnose, overvåkning og/ eller behandling på medisinsk grunnlag og som for å fungere er avhengig av en energikilde (strøm, lys, gass- eller væsketrykk) samt nødvendig tilbehør til slikt utstyr (Medisinsk Teknologisk Forening).

Normen	Norm for informasjonssikkerhet i helse- og omsorgstjenesten (Normen) er en bransjenorm utarbeidet av sektoren for sektoren. Stadig større deler av kommunikasjonen i helse- og omsorgssektoren foregår elektronisk. De utfordringer dette medfører for personvernet ble bakgrunnen for at Helsedirektoratet i 2002 tok initiativ til å utarbeide omforente regler for trygg og sikker informasjonsutveksling mellom aktørene i sektoren. Normen skal bidra til å etablere mekanismer hvor virksomhetene kan ha gjensidig tillit til at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå. Normen stiller krav som detaljerer og supplerer gjeldende regelverk. Normen er imidlertid ikke heldekkende. Helseregisterloven, personopplysningsloven og øvrig regelverk stiller enkelte krav til behandling av helse- og personopplysninger utover det som er tema for Normen. Normen er utarbeidet av representanter for helse-, omsorgs- og sosialsektoren.
Offshoring	Offshoring betyr å flytte en aktivitet fra hjemlandet til utlandet. Dersom en tjeneste tidligere ble gjennomført av en virksomhet i Norge nå gjøres av en leverandør i utlandet, er det snakk om å både outsourcing og offshoring.
Outsourcing/ tjenesteutsetting	Outsourcing/tjenesteutsetting går ut på at en organisasjon går over til å skaffe en vare eller tjeneste fra en ekstern leverandør i stedet for å levere denne selv.
Pasientinformasjon (det begrepet prosjektet bruker)	Både sensitiv informasjon og personopplysning. Personopplysning er en opplysning eller vurdering som kan knyttes til deg som enkeltperson, slik som for eksempel navn, adresse, telefonnummer, e-postadresse, IP-adresse, bilnummer, bilder, fingeravtrykk, irismønster, hodeform (for ansiktsgjenkjenning) og fødselsnummer (både fødselsdato og personnummer). Sensitive personopplysninger er opplysninger om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeninger.
Privacy Shield	Overføring av personopplysninger kan nå skje til amerikanske selskaper som slutter seg til avtaleverket Privacy Shield, og som dermed har forpliktet seg til å følge særlige regler for beskyttelse av personopplysninger. Som følge av EØS-avtalen kan Privacy Shield også benyttes som grunnlag for overføring av personopplysninger fra norske virksomheter til USA. Privacy Shield trådte i kraft 12. juli 2016, og overtar for den tidligere «Safe Harbor»-avtalen.
Regionale helseforetakene (RHF)	De regionale helseforetakene i Norge består av Helse Sør-Øst RHF, Helse Midt RHF, Helse Vest RHF og Helse Nord RHF. I tillegg til å drive sykehusene og sørge for at befolkningen blir tilbudt spesialiserte helsetjenester, har de regionale helseforetakene oppgaver innen forskning, utdanning og opplæring av pasienter og pårørende.

Sikkerhetsloven (§ 29a anskaffelser til kritisk infrastruktur)	Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). Lovens § 29a pålegger en risikovurdering ved anskaffelse av kritisk infrastruktur. Dersom risikovurderingen avdekker at anskaffelsen kan innebære en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført, skal overordnet departement varsles. Et departement som mottar varsel etter andre ledd, bør innhente en rådgivende uttalelse fra relevante organer om leveransens risikopotensial, og leverandørers sikkerhetsmessige pålitelighet. Dersom en anskaffelse til kritisk infrastruktur kan medføre en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført, kan Kongen i statsråd fatte vedtak om at anskaffelsen skal nektes gjennomført, eller om at det settes vilkår for gjennomføringen.
Skjermingsverdig informasjon	Sikkerhetsloven § 3: Informasjon som skal merkes med sikkerhetsgrad etter reglene i § 11 i loven her.
Skjermingsverdig objekt	Sikkerhetsloven § 3: eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser.
Skytjeneste og -løsninger	Skytjenester, eller Cloud Computing, er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett. De mest vanlige skytjeneste er programvare som tjeneste, plattform som tjeneste og infrastruktur som tjeneste. (Skytjenester, veiledning, 2014; Datatilsynet, s. 4). En skyløsning omfatter ofte flere ulike skytjenester som serverkapasitet, back-up og all programvare.

VEDLEGG 2:
Oversikt over aktører – deltakelse og innlegg på seminar

I dette vedlegget ligger det en oversikt over hvilke aktører som deltok i oppstartsmøte og dialogseminarene. I disse møtene fikk aktørene mulighet til å holde innlegg.

Oppstartsmøte med hovedaktørene 31. august 2017

Innlegg	
Folkehelseinstituttet ved Berit Ragnhild Svellingen	
Hamar kommune ved Marianne Bjønness	
Helse Midt RHF ved Øyvind Røset	
Helse Nord RHF ved Ida-Kristin Martinussen	
Helse Sør-Øst RHF ved Per Meinich	
Helse Vest RHF ved Lars Erik Baugstø-Hartvigsen	
Helsetjenestenes driftsorganisasjon (HDO) ved Kjetil Are Lund	
Norsk Helsenett ved André Meldal	
Pasientreiser HF ved Hilde Holt	
Sykehusinnkjøp HF ved Silje Jakola-Fjeld	
Telenor ved Hanne Tangen Nilsen	
Øvrige aktører	
Bærum kommune	KINS
Finnmarkssykehuset HF	LMT Setesdal
Helse Bergen HF	Nasjonal IKT HF
Helse Fonna HF	Nasjonalt senter for e-helseforskning
Helse Førde HF	Norsk Helsenett SF
Helse Midt-Norge IT	Oslo kommune
Helse Midt-Norge, Helseplattformen	Oslo universitetssykehus HF
Helse Møre og Romsdal HF	Stavanger kommune
Helse Nord-Trøndelag HF	Sykehusapotek Nord HF
Helse Nord, Forvaltningssenter EPJ	Sykehuset Østfold HF
Helse Stavanger HF	Sykehuspartner HF
Helse Vest IKT AS	Trondheim kommune
Helsedirektoratet	

Dialogseminar med kompetansemiljøene 7. september 2017

Innlegg (skriftlig og muntlig)	
Center for Cyber and Information Security (CCIS)	Stewart Kowalski
Datatilsynet	Veronica Jarnskjold Buer
Direktoratet for forvaltning og IKT (DIFI)	Remi Longva
Direktoratet for samfunnssikkerhet og beredskap (DSB)	Eline Palm Paxal
Helse Midt RHF (via Skype)	Øyvind Røset og Bjørn-Einar Kolstad
Helse Sør-Øst RHF	Ann-Margrethe Mydland og Heidi Thorstensen
Nasjonal kommunikasjonsmyndighet (NKOM)	Rune Kanck og Svein Scheie
Nasjonal sikkerhetsmyndighet (NSM)	Bente Hoff og Terje Aarhus

Dialogseminar med IKT-næringen 13. september 2017

Innlegg
Microsoft ved Ole Tom Seierstad
Roche Diagnostics Norge AS ved Aage Andersen
IBM ved Morten Bjørklund
DXC ved Stuart Lawrence
Vingmed AS ved Tor Havnes
Sopra Steria Lillian Røstad og Gunnar Mørne
Øvrige aktører
Abelia ved Tarje Bjørgum
Alere AS ved Terje Rybråten
B. Braun Medical AS ved Nils Arne Greftegreff
DXC – Geirr Gustavsen og Kim Mugaas
Evry – Sigurd Alfsen, Ulf Dahl Ryen, Christian Sletbak-Akerø
IBM – Karina Bjørnarøy og Loek Vredenberg
IKT Norge – Nard Schreurs og Fredrik Syversen
Medtek Norge – Trond Dahl Hansen
Medtronic AS – Erik Sturla Kongshaug
Philips Norge AS - Paolo Bernardi
Vingmed AS – Ole Einar Småkasin

Dialogseminar med fag- og pasientorganisasjoner 14. september 2017

Innlegg (presentasjon eller muntlig)
Teknologirådet ved Hilde Lovett
Datatilsynet ved Grete Alhaug
Diabetesforbundet ved Sverre Ur
Tekna ved Birgitte Jordahl
Den norske legeforening ved Eirik Nikolai Arnesen
Norsk tjenestemannslag ved Hallvard Berge
Norsk sykepleierforbund ved Jo Cranner
Den norske tannlegeforeningen ved Geir Fjerdingen
NITO ved Harald Stavn
Fagforbundet ved Christian Danielsen
Norsk Psykologforening ved Julius Okkenhaug

VEDLEGG 3:
Hvilke aktører som har bidratt med innspill til rapporten

I denne tabellen presenteres en oversikt over hvilke aktører som var delaktige i oppdragsperioden og på hvilken måte. For de aktørene som holdt innlegg under dialogseminarene var det flere som svarte direkte på problemstillingene i oppdraget under sine innlegg, mens andre aktører sendte inn skriftlige innspill i etterkant av dialogseminarene. Så selv om enkelte aktører ikke har blitt huket av på «sendt skriftlig innspill» under, så kan de allikevel ha sendt inn relevant informasjon til prosjektet ved å sende sine innlegg i etterkant.

Aktørene	Holdt innlegg under oppstartsmøte/ dialogseminar	Sendt skriftlig innspill	Sær-møter
Hovedaktørene			
Helse Sør-Øst RHF	✔	✔	✔
Helse Vest RHF	✔	✔	
Helse Midt RHF / Helseplattformen	✔	✔	✔
Helse Nord RHF	✔	✔	
Norsk Helsenett SF	✔	✔	
Nasjonal IKT	✔		
Helsetjenestenes driftsorganisasjon (HDO)	✔	✔	
Folkehelseinstituttet	✔	✔	
Sykehusinnkjøp HF	✔	✔	
Pasientreiser HF	✔	✔	
Trondheim kommune		✔	
Hamar kommune	✔		
Sandefjord kommune		✔	
Bærum kommune		✔	
LMT Setesdal (Bykle, Valle, Bygland og Evje og Hornnes)		✔	
Kompetansemiljøer 7.9			
Center for Cyber and Information Security (CCIS)	✔		
Datatilsynet	✔		✔

Aktørene	Holdt innlegg under oppstartsmøte/ dialogseminar	Sendt skriftlig innspill	Sær-møter
Direktoratet for forvaltning og IKT (DIFI)	✔	✔	
Direktoratet for samfunnssikkerhet og beredskap (DSB)	✔		
Nasjonal sikkerhetsmyndighet (NSM)	✔	✔	✔
Nasjonal kommunikasjonsmyndighet (NKOM)	✔		
IKT-næringen 13.9			
DXC	✔	✔	
Evry			
IBM	✔	✔	
IKT Norge		✔	
Medtek Norge		✔	
Microsoft	✔		
Philips Norge AS			
Roche Diagnostics AS	✔		
Vingmed AS	✔		
Sopra Steria	✔	✔	
Fag- og pasientorganisasjoner 14.9			
Datatilsynet	✔		
Teknologirådet	✔		
Fagforbundet	✔	✔	
Den norske legeforening	✔	✔	
NITO	✔	✔	
Tekna	✔	✔	
Norsk sykepleierforbund	✔	✔	
Diabetesforbundet	✔		
Norsk tjenestemannslag	✔		
Den norske tannlegeforening	✔		
Norsk psykologforening	✔		
Særmøter			
Pasient og brukerombud i Sogn og Fjordane og Oslo			✔
Apotekerforeningen			✔
Fastleger (deltakende i EPJ-løftet)		✔	✔
NUFA (Fagutvalget)			✔
Statoil			✔

Alle aktørene fikk tilsendt beskrivelsen av oppdraget, inkludert de fire del-leveransene. Tabellen nedenfor viser konkretisering av spørsmålene stilt til de ulike aktørene og som de fikk mulighet til å besvare.

Aktører	Spørsmål
Hovedaktørene RHFene, Helsenett, HDO, Folkehelseinstituttet, Pasientreiser og kommuner	Totalt 19 spørsmål fordelt på fem områder skulle besvares (se spørreskjemaet i vedlegg 4). Disse områdene er: • Del I – Generelt om bruk av tjenesteutsetting til private leverandører • Del II – Bruk av tjenesteutsetting til private leverandører • Del III – Kriterier ved bruk av tjenesteutsetting til private / bruk av private leverandører • Del IV – Rutiner ved tjenesteutsetting til private/ bruk av private leverandører • Del V – Avveininger
Sykehusinnkjøp HF og Nasjonal IKT	• Hvilke hovedutfordringer og barrierer er tilstede ved bruk av private leverandører? • Hvilke endringer kan være nødvendige for å gjøre det mulig å bruke det private leverandørmarkedet på en sikker og effektiv måte?
Kompetansemiljøene	• Foreslå gode rutiner for å sikre at de til enhver tid gjeldende krav til informasjonssikkerhet ved bruk av private leverandører etterleves • Status for bruk av nasjonale og internasjonale leverandører av tjenester som kontinuerlig eller episodisk arbeider inn mot virksomhetens datasystemer og under hvilke betingelser dette skjer. • Kriterier eller betingelser som bidrar til at denne formen for tjenester skjer på en ansvarlig måte og i tråd med de til enhver tid gjeldende krav. • Er det tjenester som ikke bør settes ut til private leverandører? Bør det skilles mellom ulike jurisdiksjoner (Norge, EØS, globale)?
IKT-næringen	• Hvilke hovedutfordringer og barrierer er tilstede ved bruk av private leverandører i helse- og omsorgsektoren? • Hvilke endringer kan være nødvendige for å gjøre det mulig å bruke det private leverandørmarkedet på en sikker og effektiv måte? • Er det tjenester som ikke bør settes ut til private leverandører? Bør det skilles mellom ulike jurisdiksjoner (Norge, EØS, globale)?
Fag- og pasientorganisasjoner	• Hvilke kriterier, betingelser og tiltak anser organisasjonene som nødvendig for å kunne benytte private underlevererandører på en trygg og ansvarlig måte? • Er det tjenester som ikke bør overlates til private underleverandører, og hvilke kriterier legger en til grunn for denne anbefalingen?

VEDLEGG 4: Spørreskjemaet

Denne spørreundersøkelsen ble sent ut til alle de regionale helseforetakene (RHFene), noen kommuner, Norsk Helsenett, HDO, Folkehelsedirektoratet og Pasientreiser. I etterkant ble spørsmål 4 b inkludert i spørreskjemaet, dette spørsmålet svarte kun de regionale helseforetakene på.

Informasjonssikkerhet ved bruk av private leverandører innen IKT-området

Direktoratet for e-helse har fått i oppdrag fra Helse- og omsorgsdepartementet å gjennomgå informasjonssikkerhet ved bruk av private underleverandører i helse- og omsorgssektoren.

Denne informasjonshentingen skal brukes til å utarbeide en status på håndteringen av informasjonssikkerhet ved bruk av private IKT-leverandører i helse- og omsorgstjenesten, samt gi mulighet for innspill til hva som skal til for å sikre en trygg og riktig bruk av både nasjonale og internasjonale leverandører av løsninger og tjenester. Informasjonssikkerhet dekker om pasientinformasjon og avgrenses til problemstillinger rundt sikkerhet ved bruk av private leverandører og dekker områdene IT-drift, applikasjonsforvaltning og applikasjonsutvikling hvor man får tilgang til pasientinformasjon. Vi ønsker å dekke både mer omfattende tjenesteutsetting og mindre/tidsavgrensede tjenesteavtaler. Dette inkluderer problemstillinger rundt medisinsk teknisk utstyr.

Informasjonsinnhenting er sendt til alle RHF-er, noen kommuner og aktører.

Dersom dere har spørsmål eller innspill til denne forespørselen kontakt Jan Gunnar Broch (e-post: Jan.Gunnar.Broch@ehelse.no) eller Tore Magnussen (e-post: tma@a-2.no).

Svarfrist er 12. september 2017.

Informasjon om informasjonsinnhentingen

Vi understreker at denne informasjonsinnhentingen skal gi en overordnet status for bruk av nasjonale og internasjonale leverandører som en del av oppdraget med å identifisere og forelå gode rutiner for etterlevelse av krav til informasjonssikkerhet. Vi spør også generelt om kriterier, krav og rutiner som en del av dette arbeidet.

Totalt er det **19 spørsmål** fordelt på **fem område**r som skal besvares. Disse områdene er:

- Del I – Generelt om bruk av tjenesteutsetting til private leverandører
- Del II – Bruk av tjenesteutsetting til private leverandører
- Del III – Kriterier ved bruk av tjenesteutsetting til private / bruk av private leverandører
- Del IV – Rutiner ved tjenesteutsetting til private/ bruk av private leverandører
- Del V – Avveininger

Del II til V omhandler primært pasientinformasjon

Påse at du besvarer alle spørsmål som er relevante for din sektor. De fleste spørsmålene krever noe lengre svar, mens i enkelte spørsmål ønsker vi at dere f.eks. svarer en prosentandel. Når det gjelder prosentandel og størrelser er vi ute etter anslag på omfang. Vi ønsker gjerne status per dato.

På spørsmål med korte svar ønsker vi at dere i tillegg gir en kommentar med tanke på hvordan dere har kommet frem til svaret.

Når vi i det etterfølgende bruker ordet «pasientinformasjon» mener vi helse- og personopplysninger knyttet til navngitte eller identifiserbare pasienter og/eller brukere.

Hvilken virksomhet gjelder besvarelsen for?

Vennligst skriv inn: _____

Del I – Generelt om bruk av tjenesteutsetting til private leverandører

1. I hvor stor grad er IKT-tjenester levert av private leverandører innen følgende områder (anslå i % andel av totalkostnader for det enkelte område):

- Basisdrift (omfatter drift av datasentertjenester, nettverk, lagring og back-up, OS-drift, drift av databaser og mellomvare inkludert medisinsk-teknisk utstyr, IT brukerstøtte, drift av arbeidsplassutstyr): _____
- Applikasjonsdrift (drift av dataløsninger): _____
- Applikasjonsforvaltning (som feilretting og nye versjoner): _____
- Applikasjonsutvikling (ny funksjonalitet): _____

Del II – Bruk av tjenesteutsetting til private leverandører

2. I hvor stor grad er basisdrift av infrastruktur og plattform for systemer med pasientinformasjon i dag levert av private leverandører (dette omfatter drift av datasentertjenester, nettverk, lagring og back-up, OS-drift, drift av databaser og mellomvare inkludert medisinsk-teknisk utstyr, IT brukerstøtte, drift av arbeidsplassutstyr)? Anslå i % den andel av de nevnte tjenestenes totale kostnader som går til private leverandører.

Svar i prosent:
Kommentar:

3. I hvor stor grad er applikasjonsdrift (drift av dataløsninger) for systemer med pasientinformasjon i dag levert av private leverandører? Anslå i % den andel av de nevnte tjenestenes totale kostnader som går til private leverandører.

Svar i prosent:
Kommentar:

4 a. I hvor stor grad er applikasjonsforvaltning (som feilretting og nye versjoner) av systemer med pasientinformasjon i dag levert av private leverandører (dette gjelder både fjernaksess og fysisk tilstedeværelse)? Anslå i % den andel av den nevnte tjenestenes totale kostnader som går til private leverandører.

Svar i prosent:
Kommentar:

4 b. *I hvor stor grad har ansatte hos eksterne private leverandører som jobber med applikasjonsforvaltning tilgang til pasientinformasjon?*

☐ *Aldri*
☐ *I liten grad*
☐ *I noen grad*
☐ *I stor grad*
☐ *I svært stor grad*

(Dette spørsmålet var ikke i den opprinnelige spørreundersøkelsen, men ble lagt til i etterkant for de regionale helseforetakene)

5. I hvor stor grad har ansatte hos eksterne applikasjonsutviklere tilgang til pasientinformasjon, f.eks. i forbindelse med test, migrering og mindre utviklingsoppdrag?

☐ *Aldri*
☐ *I liten grad*
☐ *I noen grad*
☐ *I stor grad*
☐ *I svært stor grad*

Gi en kommentar om hvor dette primært skjer.

Kommentar:

6. Er det noen områder i dag hvor det benyttes eksterne skytjenester hvor det behandles pasientinformasjon. Angi områder.
(Spørsmålet er overlappende med omfanget i spørsmålene 2–5, men vi ønsker en oversikt over områdene).

Svar:

7. I hvor stor grad har private leverandører av medisinsk-teknisk utstyr tilgang til pasientinformasjon, f.eks. via intern aksess, fjern aksess eller ekstern lagring av data? Beskriv også omfang og på hvilke områder slik tilgang benyttes.

Svar:

8. Hvilke erfaringer (positive og negative) har dere med de private leverandørene og avtalene dere har med dem? Har dere vært fornøyd med hvordan informasjonssikkerheten har ivaretatt? Har det vært utfordringer eller hendelser rundt uautorisert tilgang til pasientinformasjon, og hvilke tiltak er eventuelt blitt igangsatt?

Svar:

9 a) Hvis det er personell hos leverandørene og deres underleverandører som må få tilgang til pasientinformasjon, i hvilket land befinner dette personellet seg? Kryss av for aktuelt land, og angi anslag for prosentandel for alle private leverandører:

Land	Prosentandel for alle private leverandører
☐ Norge	
☐ EØS	
☐ Utenfor EØS	

Kommentar:

b) Dersom land utenfor EØS ble krysset ut, angi land, omfang og hvilke tjenesteområder det gjelder.

Svar:

Del III – Kriterier ved bruk av tjenesteutsetting til private / bruk av private leverandører

Når det gjelder medisinsk-teknisk utstyr, ønsker vi kommentarer der det er relevant.

10. Ved bruk av private leverandører hvilke kriterier ser dere som de viktigste for å bestemme hvilke systemer og tjenester de kan levere? Dette inkluderer også underleverandører. (Eksempel på kriterier er tilgjengelighet kompetanse og kapasitet, kostnader, ny teknologi, alternative/nye leveransemodeller som f.eks. skytjenester).

Svar:

11. Dersom dere verken benytter private leverandører eller har vurdert dette, vennligst oppgi grunner for dette.

Svar:

12. Når dere har besluttet å benytte privat leverandør for en tjeneste for et system, hvilke krav må oppfylles av leverandør/underleverandør rundt sikring av pasientinformasjon? Har dere vurdert andre sikkerhetshensyn enn sikring av pasientinformasjon? Hvilke tiltak må være iverksatt av egen organisasjon før tjenesten settes ut? (Eksempler er teknisk, arkitektur-messig, organisatorisk, rutiner). Angi svaret med tanke på både historiske og pågående prosesser.

Svar:

13. Er det tjenester som dere mener ikke bør overlates til private leverandører? Er det jurisdiksjoner (land) som enkelte tjenester ikke bør settes ut til private leverandører? Begrunn eventuelt hvorfor dere mener dette ikke bør settes ut eller leveres fra eksterne private leverandører?

Kommenter nedenfor per tjenesteområde, eventuelt hvilke deler av tjenesteområder, som ikke bør overlates til private leverandører. Kommenter eventuelt begrensninger vedrørende jurisdiksjoner (land).

Svar vedrørende basisdrift: _____
Svar vedrørende applikasjonsdrift: _____
Svar vedrørende applikasjonsforvaltning: _____
Svar vedrørende applikasjonsutvikling (migrasjon, test, driftssetting): _____

Andre kommentarer:

14. Hvis dere benytter private leverandører som skal ha tilgang til pasient-informasjon, hvilke jurisdiksjoner (land) krever dere at leverandørene og leverandørenes personell kan holde til i? Angi svaret med tanke på både historiske og pågående prosesser.

☐ Norge
☐ EØS
☐ Annet, vennligst angi land: _____

Kommentar:

15. Hvilke innspill til endringer i nåværende krav har dere, for å bidra til at denne formen for tjenester skjer på en ansvarlig måte?

Svar:

16. Hvilke utfordringer er tilstede ved bruk av private leverandører? Hvilke endringer kan være nødvendige for å gjøre det mulig å bruke det private leverandørmarkedet på en sikker og effektiv måte? Relater det gjerne til nye tjenester og leveransemåter.

Svar:

Del IV – Rutiner ved tjenesteutsetting til private/ bruk av private leverandører

17. Hvilke rutiner har dere for å sikre at kriteriene vedrørende informasjons-sikkerheten til pasientopplysning blir oppfylt per prosess under:

- Anskaffelsesprosessen – blant annet sikre at kriteriene blir oppfylt, og at kravene til leverandør blir avtalefestet?
  Svar:
- Implementering/overføring (før driftsettelse) – blant annet sikre at kriteriene blir oppfylt og at interne tiltak blir iverksatt i tide?
  Svar:
- Oppfølging av løpende «drift» – blant annet sikre at kriteriene blir oppfylt og at interne tiltak blir iverksatt i tide?
  Svar:

18. Hvilke forbedringer/endringer i rutiner ser dere som hensiktsmessige for å sikre etterlevelse av krav til informasjonssikkerhet ved bruk av private leverandører?

Svar:

Del V – Avveininger

19. Ved fastsettelse av kriterier, krav og rutiner, hvilke vurderinger og avveininger mellom risiko/sårbarhet og effekter (kostnader og gevinster) av utsettingen til eller bruk av privat leverandør er gjort?

Svar:

VEDLEGG 5:
Risikoreduserende tiltak ved tjenesteutsetting

Risikovurdering er helt sentralt ved tjenesteutsetting av IKT. Risikovurderingen handler ikke bare om å identifisere og kvantifisere sårbarheter og trusler, men også om å identifisere, vurdere og planlegge risikoreduserende tiltak. I dette vedlegget vil vi se nærmere på det siste. Dette finnes tekniske tiltak som både kan redusere sannsynlighet for brudd på informasjonssikkerheten og redusere konsekvensen av eventuelle brudd. Innen helse- og omsorgssektoren er det spesielt to typer tekniske tiltak som har vært benyttet: perimetersikring og applikasjonssikkerhet. Dette er viktige tiltak, men de reduserer i beskjeden grad risiko i forbindelse med tjenesteutsetting av IKT. Det finnes derimot mange andre tiltak som gjør det. . Dette ble kort nevnt i rapportens kapittel 6.2 og 6.3. Her blir tiltakene beskrevet i mer detalj.

Mulig risikoreduserende tiltak ved tjenesteutsetting

Det er en rekke tiltak man kan gjøre for å redusere risiko. Det dreier seg om forebyggende tiltak som:

- Å **avskrekke** eventuelle angripere
- Å **beskytte** systemene

Det dreier seg også om beredskapstiltak som gir en bedre håndtering av hendelser når de likevel inntreffer som

- Å **oppdage** dem
- Å **håndtere** hendelsene raskt og godt
- Å **gjenopprette** en sikker tilstand

God informasjonssikkerhet krever både forebygging og beredskap. Tiltakene kan deles inn i tre typer

- Fysisk
- Teknisk
- Organisatorisk

Fysiske tiltak dreier seg om fysisk sikring av utstyr både mot angrep og mot det fysiske miljøet. Eksempler på fysisk sikring er solide vegger og dører, låser, kameraovervåkning, vakthold, overspenningsvern og flomvern. Redundans gir mer robuste løsninger ved å sikre at det ikke er noe enkelt punkt som gir svikt alene, for eksempel ved å ha dobbelt opp av utstyr og linjer og datasentre på ulike lokasjoner.

Tekniske tiltak (også kjent som logiske) dreier seg om sikkerhet bygd inn i systemene som identitet- og tilgangsstyring, kryptering, logging osv.

Organisatoriske tiltak (også kjent som administrative) dreier seg om sikkerhet knyttet organisasjonen og personell i organisasjonen som bakgrunnssjekker, kompetanse, kultur, avtaler, kontrollrutiner osv.

De tre typene tiltak henger sammen. Man kan til en viss grad bruke tiltak av en type for å kompensere for manglende tiltak av en annen type. Et eksempel er når datasenter deles med andre. Da kan ikke alltid fysisk tilgang begrenses til eget utstyr og til eget autorisert personell. For å kompensere for dette kan data som er lagret på utstyret og som transporteres mellom det krypteres, slik at informasjonen er i en form som gjør den vanskelig tilgjengelig for dem med fysisk tilgang.

Tjenesteutsetting av IKT forutsetter tekniske tiltak som ofte ikke er på plass

Tjenesteutsetting av IKT har konsekvenser for informasjonssikkerheten. Det organisatoriske miljøet vil nødvendigvis endre seg siden man går fra å ha produksjonen internt i organisasjonen styrt gjennom organisasjonens interne styringssystem til å skje delvis i ett eller flere andre foretak styrt gjennom avtaler og samarbeid. Man har ikke lenger direkte styringsrett av personell som utfører arbeid for organisasjonen.

Selv med de beste avtaler vil man miste noe organisatorisk kontroll ved tjeneste-utsetting. Dette betyr at man gjerne må bruke noen andre typer tiltak for å kompensere. Tjenesteutsetting har ofte også ofte direkte konsekvenser for det fysiske og det tekniske. Tjenestene leveres gjerne fra andre steder og ved hjelp av annet utstyr og systemer enn det som ellers ville vært tilfellet.

Mange av IKT-løsningene i helsesektoren ble utviklet og designet i en tid da tjenesteutsetting av IKT i sektoren ikke var et tema. Dette har hatt konsekvenser for hvordan man har valgt å sikre systemene. Tradisjonelt har de tekniske til-takene i hovedsak dreid seg om perimetersikring og applikasjonssikring.

Perimetersikring består i hovedsak å bygge hindre i nettverket ved hjelp av brannmurer og lignende. Man deler gjerne verden inn i soner og begrenser tilganger ut i fra det. Et enkelt eksempel kan for eksempel være slik:

- Åpen sone – Alle på Internett er i denne sonen. Her kan man få tilgang til de offentlige nettsidene til foretaket og eventuelle selvbetjeningsløsninger det tilbyr.
- Intern sone – Alle ansatte og innleide på det lokale nettverket eller fra annet sted ved hjelp av løsning for fjernoppkobling er i denne sonen. De kan i tillegg nå applikasjoner rettet mot interne brukere i foretaket.
- Driftssone – Her har bare IKT-driftspersonell tilgang. De får her direkte tilgang til tjenerne som brukes til å levere applikasjonene.

Det var et svært enkelt eksempel og ofte har man langt flere soner for å gi en mer finmasket kontroll. For eksempel kan man ha ulike driftssoner slik at de som

driver med applikasjonsdrift bare for tilgang til de tjenerne som brukes av sine applikasjoner eller man kan ha en egen «sikker» sone som gir tilgang til applikasjoner med informasjon som skal behandles fortrolig.

Ved tjenesteutsetting av IKT-tjenester, spesielt driftstjenester, må man slippe eksternt personell inn i de mest begrensede sonene for at de skal kunne utføre arbeidet sitt. Dette gjelder både basis- og applikasjonsdrift. For applikasjonsdrift kan man begrense tilgang til infrastrukturen til en bestemt applikasjon ved å lage egne soner for dem.

Applikasjonssikring dreier seg om å sikre applikasjonene herunder identitet- og tilgangsstyring for brukere, ulike former for sporing og kryptering av forbindelsen fra tjener til klient. Dette er på plass i mange kliniske systemer i dag.

Ved tjenesteutsetting av IKT-tjenester har applikasjonssikring begrenset verdi som risikoreduserende tiltak. IKT-personell må gjerne ha tilgang direkte til infrastruktur, plattform og applikasjonskomponenter på tjenere og kommer da utenom tradisjonell applikasjonssikring.

Finnes tekniske tiltak som begrenser risiko ved tjenesteutsetting av IKT

Det finnes tekniske tiltak som begrenser risiko ved tjenesteutsetting av IKT. Det dreier seg om verktøy man kan ta i bruk og endringer i hvordan applikasjonene er satt sammen, deres arkitektur, som gjør det mulig å bruke disse verktøyene.

Identitet- og tilgangsstyring for privilegerte brukere

IKT-personell omtales ofte som privilegerte brukere siden de har langt mer omfattende tilganger enn andre brukere og siden tilgangene gjerne går utenom applikasjonssikkerhet.

Identitet- og tilgangsstyring handler om å sikre at de rette personene har tilgang til de rette ressursene til de rette tidene. Systemer for identitet og tilgangs-styring tilbyr verktøystøtte for dette. De gir:

- Sentral oversikt over identiteter – hvem det er snakk om
- Kontroll på at personer er dem de gir seg ut for å være, autentisering
- Håndtering av hvilke tilganger hvem skal ha nå, autorisasjon

Med verktøy for identitet- og tilgangsstyring får man en sentral oversikt over identiteter, kontoer, tilganger og bruken av disse. Dette gjør det enklere å administrere og å kontrollere tilganger. Uten en slik sentral oversikt vil det kreve mye tid og innsats å gjennomføre periodiske gjennomganger av tilganger og å foreta revisjoner og tilsyn. Det gjør det også vanskelig å kontrollere at brukere ikke har ulovlige kombinasjoner av tilganger, situasjoner av typen «bukken og havresekken». For eksempel bør ikke personell som har tilgang til å administrere

et system også ha tilgang til å administrere systemet for logging av hva som gjøres på tjenerne.

Identitet

Ved tjenesteutsetting av IKT-tjenester er identitet knyttet til leverandørene, deres underleverandører og personell hos disse. For norske leverandører som leverer tjenestene fra Norge er ikke dette så vanskelig. Vi har sentrale oversikter og identifikatorer for både fysiske og juridiske personer. Fysiske personer finnes i Det sentrale folkeregister og er unikt identifisert ved hjelp av deres fødsels- eller D-nummer. Juridiske personer finnes i Foretaksregisteret og er unikt identifisert ved hjelp av deres organisasjonsnummer. I noen andre land finnes det tilsvarende, men ikke i alle. Selv der det finnes, er det ikke sikkert at man uten videre får tilgang til dem eller at det er lett å gjennomføre i praksis.

Knyttet til identitet for fysiske personer kan det være nyttig å få informasjon om blant annet:

- Nasjonalitet
- Ansettelsesforhold som arbeidsgiver, stilling og arbeidssted
- Taushetserklæringer
- Bakgrunnssjekker
- Sikkerhetsklarering

Knyttet til identitet for juridiske personer som aksjeselskap og lignende kan det være nyttig å ha informasjon om blant annet avtaler om tjenesteutsetting av IKT, databehandleravtaler og sikkerhetsavtaler.

Autentisering

Systemer som brukes ved levering av helsehjelp havner fort oppe i det øverste risikonivået i Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor[1] siden det potensielt kan forekomme tap av liv og/eller store helseskader. Dette nivået, risikonivå 4, medfører krav om sikkerhetsnivå 4 – to-faktorautentisering hvorav én skal være dynamisk.

To-faktorautentisering betyr at det kreves to ulike faktorer for autentisering. En faktor kan være:

- Noe du vet, som for eksempel PIN-kode eller passord
- Noe du er, som for eksempel fingeravtrykk eller ansiktstrekk
- Noe du har, som et smartkort eller en passordkalkulator

Det at én av faktorene skal være dynamisk betyr at den endres fra gang til gang. Eksempler på slike løsninger er tidsbaserte passordkalkulatorer, som gir nytt passord avhengig av tid, og løsninger basert på PKI, hvor det ved hver autentisering genereres en ny, tilfeldig datastreng som signeres digitalt.

1 https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/

I Norge har vi en etablerte fellesløsning på sikkerhetsnivå 4 som Bank ID, Buypass og Commfides. Det finnes tilsvarende i noen andre land og det finnes EU-standarder som skal gi interoperabilitet, men i praksis er det en tilleggs-utfordring når man har personell i utlandet.

Systemet kan også kreve at man autentiserer seg på nytt etter en tids inaktivitet for å hindre at uvedkommende for tilgang ved å bruke noen andres utstyr som har blitt forlatt uten å ha blitt låst.

Autorisasjon

Med systemer for identitet- og tilgangsstyring er det mulig å automatisk håndheve bestemmelser for når og hvor man skal ha tilgang. Man kan for eksempel sette opp regler som er spesielt relevante ved tjenesteutsetting som at:

- Man ikke skal ha tilganger som gjør at man kan se personopplysninger hvis man ikke har undertegnet en taushetserklæring og er ansatt i et foretak man har en databehandleravtale med.
- Man ikke skal ha tilganger som gjør at man kan se gradert informasjon hvis man ikke er sikkerhetsklarert og er ansatt i et foretak man har en sikkerhets-avtale med.
- Man ikke skal ha tilgang fra ikke-godkjente steder, utstyr eller nettverk.
- Man skal ikke ha tilgang med mindre man har en aktiv arbeidsoppgave som tilsier at det er nødvendig med tilgang.

Ved tjenesteutsetting får man tilleggsutfordringer med autorisasjon. Det kan være vanskelig for internt personell å bedømme hvorvidt en person hos en leverandør har tjenstlig behov for en tilgang. Dette forutsetter at man vet og forstår hvordan leverandøren er organisert, hvilke arbeidsoppgaver de enkelte hos leverandøren har og hva de krever av tilganger. Dette er krevende oppgaver både ved forespørsel om tilganger og ved periodiske gjennomganger av tilganger. For internt personell har man både tilgang til personalsystemet som inneholder denne informasjonen og kan hvile seg på nærmeste leder som har de beste forutsetningene for å forstå arbeidsoppgavene til sine medarbeidere. Det at disse oppgavene er såpass krevende gjør at man både risikerer forsinkelser og at vurderingene ikke blir reelle.

Systemet må også håndtere tilganger i forbindelse med uønskede hendelser. Det kan være at man havner i en situasjon med kritiske eller alvorlige feil der eget personell ikke er i stand til å løse problemet og har behov for bistand fra ekstern ekspertise. Ved slike situasjoner må systemet gjøre det raskt å gi tidsbegrenset tilgang til personell som normalt ikke skulle ha det, men på en måte som gjør at man i etterkant kan se at det ble gjort og hvorfor. Informasjonssikkerhet dreier seg ikke bare om konfidensialitet, men også om tilgjengelighet.

Provisjonering

Det hjelper ikke å ha et system for privilegert identitet- og tilgangsstyring hvis ikke løsningene man har forøvrig fungerer med det. Det å la en slik sentralt system spre de nødvendige brukerkontoene og tilgangene til andre systemer kalles provisjonering og det finnes standarder for det. Det er imidlertid ikke alle som støtter disse standardene, spesielt ikke eldre løsninger. Der det mangler støtte krever det mer å få på plass sentral identitet- og tilgangsstyring. Det er ikke alltid mulig å gjøre det på en måte som supporteres av leverandørene.

Føderasjon

Som vi har sett kan identitet, autentisitet og autorisasjon være utfordrende å få til for eksternt personell, spesielt i utlandet. En mulig løsning er i stedet å benytte leverandørens egne løsninger. Hvis leverandøren har gode nok tekniske løsninger og administrative rutiner, kan man ved hjelp av noe som heter føderasjon gjøre det mulig for eksternt personell å bruke sin arbeidsgivers løsning for å logge seg på.

For at dette skal være aktuelt, må man før man setter det opp vurdere om løsningene er pålitelige nok, både teknisk og administrativt, og man må etter implementering kontrollere at det fungerer som avtalt og gjennomføre nødvendige forbedringer som konsekvens av endringer i risikobildet.

Sikre forbindelser og arbeidsflater

Ofte vil eksternt personell arbeide på utstyr og fysiske steder som ikke kontrolleres av kunden. Dette medfører økt risiko siden man ikke selv kan sikre utstyret og nettverket fysisk. Noe av dette kan til dels kompenseres ved administrative tiltak som avtaler som stiller krav om fysisk sikring av arbeidsplass, kryptering av disker og verktøy for å oppdage ondsinnet programvare, samt kontroller av at disse etterleves.

For å hindre avlytting og manipulasjon av kommunikasjon over samband finnes det tekniske tiltak som ved hjelp kryptering etablerer virtuelle private nettverk. I helse- og omsorgssektoren i Norge har man et felles slik nettverk kalt Helsenettet som leveres av Norsk helsenett og i henhold til Normen bør dette benyttes.

I tillegg kan man begrense risikoen knyttet til fremmed utstyr ved å bruke terminaltjenere. Personell arbeider da på en arbeidsflate levert fra en tjener hos kunden. Det gjør at data ikke lagres lokalt på utstyret og begrenser mulighetene for ondsinnet programvare å få tilgang. Terminaltjenere kan settes opp slik at det ikke er mulig å kopiere filer og elementer på utklippstavlen til og fra eget utstyr og terminalen.

Det er ikke alltid det er mulig med alle disse begrensningene. Det kan være at eksternt personell har tjenstlig behov for å kunne overføre filer som for

eksempel ved filer med oppdateringer og oppgradering av programvare eller behov for å laste ned data fra utstyr til analyse på egne tjenere.

Kryptering og signering

Det finnes også tekniske tiltak som reduserer risiko for at data kommer på avveie eller blir manipulert. Man kan for eksempel gjøre det vanskeligere for personell med fysisk tilgang til utstyr og nettverk til å misbruke disse tilgangene ved å kryptere av filsystemet på tjenerne og all kommunikasjon mellom dem på transportnivå. De vil fortsatt ha tilgang til dataene, men de vil være på en form som gjør det vanskelig å nyttiggjøre seg dem.

Dette tiltaket vil imidlertid ikke hjelpe mot driftspersonell som har mulighet for å logge seg på tjenerne. For at de skal fungere vil for eksempel operativsystemet være nødt til å dekryptere dataene lagret på filsystemet når de aksesseres. Det finnes imidlertid tekniske tiltak basert på kryptografi som gjør at denne typen driftspersonell heller får tilgang til ukrypterte data. Filer, databaser og meldinger kan også krypteres. Et eksempel på at dette er gjort er Kjernejournal der drifts-personell ikke uten videre har tilgang til dataene i databasen.

Det er også mulig å bruke kryptografi for å sikre integriteten av dataene selv når de er tilgjengelige ved hjelp av digitale signaturer og blokkjeder. Et eksempel på bruk av elektroniske signaturer i sektoren er resepter som signeres elektronisk av leger.

Disse tiltakene kan være vanskelig å få til med gamle løsninger som ikke er designet med tanke på det. Kryptering gir også dårligere ytelse og kan gjøre det vanskeligere gjenopprette data.

Anonymisering, aggregering og pseudonymisering

Det er mange situasjoner det er ønskelig med tilgang til reelle data fra produksjon som kan inneholde personopplysninger. I forbindelse med testing av systemer kan det være krevende å lage tilstrekkelige omfattende og representative testdata fra grunnen av. Leverandører av medisinsk-teknisk utstyr som blodsukkermålere kan ha behov for å ha tilgang til dataene for å gjøre dem tilgjengelige for brukeren, deres pårørende og for å formidle dem til helse-vesenet. I forbindelse med forskning og annen bruk av maskinlæring har man behov for reelle data til å teste hypoteser og å trene algoritmer.

Det finnes tekniske tiltak som kan redusere risikoen. Dataene kan for eksempel på ulike vis anonymiseres og aggregeres. Formålet med bruk av dataene er ofte ikke slik at det er nødvendig å vite hvem de gjelder. Anonymisering dreier seg om å gjøre det umulig å spore dataene tilbake til en enkelt person. Dette er vanskeligere enn bare å fjerne fødselsnummer og navn. Det kan være direkte identifiserbar informasjon i fritekstfelt og vedlagte dokumenter. I tillegg er det ofte mulig å finne ut hvem det dreier seg om ved å samkjøre opplysningene med andre datakilder. Ofte kan opplysninger som kan være relevante for for-

målet som alder og bosted være nok til å finne ut hvem noen er. Aggregering er da et annet teknisk tiltak som kan benyttes der man ikke får data om den enkelte person, men kun oppsummert for grupper av personer.

En teknikk beslektet med anonymisering er pseudonymisering. Der fjerner man også informasjon som er direkte identifiserbar, men man beholder en oversikt som gjør det mulig å finne tilbake til hvem det dreier seg om. Denne oversikten skjermes fra de som behandler dataene. For eksempel kan man tenke seg at man angir en i seg selv intetsigende token i stedet for fødselsnummer for å identifisere en pasient man kobler til noe medisinsk-teknisk utstyr. Denne brukes av utstyret for å oversende informasjon til kurve- og journalsystem som finner ut hvem det dreier seg om og legger det til rett pasient.

Det er nødvendig med verktøystøtte for å få til disse teknikkene på en god måte.

Sporing

Sporbarhet er et viktig prinsipp innen informasjonssikkerhet og dreier seg om å ta vare på informasjon om hvem som gjorde hva når og hvilke tilganger de benyttet. Dette kan blant annet brukes til etterkontroll, etterforskning og i forbindelse med periodiske gjennomganger, revisjon og tilsyn. For eksempel kan det at noen ikke har benyttet en tilgang på lang tid være en indikasjon på at vedkommende ikke lenger trenger tilgangen og den kan fjernes.

Det tekniske tiltaket er logging og verktøy for analyse av logger. Det er viktig å sikre lagringen av loggene. Det må settes opp skiller slik at personell og helst ikke annet personell hos samme leverandør har mulighet for å manipulere loggen. Det er også viktig å ta vare på loggene tilstrekkelig lenge. Avanserte angripere som etterretningsorganisasjoner kan ha angrep som går over måneder. Det kan også gå tid før man oppdager et angrep og man må ha mulighet for å gå tilbake i tid for å sikre bevis. Loggene blir fort så omfattende at man er avhengig av å verktøy for å håndtere og analysere dem.

En utfordring med å få på plass god logging er at eksisterende løsninger ikke alltid er designet med tanke på dette. En annen utfordring er at også personell hos leverandører har krav på personvern og det er begrensninger i hvor mye og hvordan man kan overvåke.

Deteksjon

Et annet mulig teknisk tiltak er å implementere verktøy som bidrar til å avdekke sårbarheter og mulige brudd på sikkerheten.

Det finnes verktøy som avdekker mulige angrep fra innsidere. Disse ser for eksempel etter uventede endringer i bruksmønster. En utfordring med disse verktøyene er at det krever mye tuning for å unngå for mange falske positiver.

Det finnes også ulike verktøy som ser etter sårbarheter for eksempel ved skanne etter kjente sikkerhetshull eller ved å se gjennom kildekode etter usikker koding som åpner for noen vanlige angrepsteknikker.

Håndtering av endringer og hendelser

Til slutt finnes det tekniske tiltak som hjelper ved håndtering av endringer og hendelser. For endringer finnes det sakssystem som gjør det mulig:

- Å planlegge hvem som skal gjøre hva når.
- Å dokumentere hva endringene går ut på og eventuelle risikovurdering (pålagt ved endringer som kan medføre konsekvenser for informasjonssikkerheten).
- Å sikre at risikovurderinger og godkjenninger er gjennomført.

Disse kan henge sammen med andre verktøy for konfigurasjonsstyring som dokumenterer hva man har med versjoner og andreegenskaper.

Det finnes også verktøy for håndtering av kritiske hendelser når de først inntreffer. Når man arbeider distribuert, som ofte er tilfellet ved tjenesteutsetting, er det ikke så lett å samle alle i et «situasjonsrom» for å sikre rask og effektiv kommunikasjon med alt relevant personell.

VEDLEGG 6:
Aktørers vurdering av hvilke tjenester som ikke bør overlates til private leverandører

I dette vedlegget gjengis aktørenes vurdering på spørsmålet om det er noen tjenester som ikke bør overlates til private leverandører, spesifisert hvilke tjenesteområder som eventuelt ikke bør settes ut, hvorvidt det burde skille mellom ulike jurisdiksjoner (Norge, EØS/EU, globale) og eventuelt kriterier som ligger til grunn for denne vurderingen.

Nedenfor presenteres en oversikt over hvilke aktører som fikk hvilke spørsmål, før vurderingene for hver aktør presenteres.

Aktører	Hvilke tjenester bør ikke overlates til private leverandører	Spesifisere hvilke tjenesteområder som eventuelt ikke bør settes ut (basisdrift og applikasjonsområder)
RHFene, Norsk Helsenett, HDO, Folkehelseinstituttet og Pasientreiser[2]	✔	✔
Kompetansemiljøene	✔	
IKT-næringen	✔	
Fag- og pasientorganisasjoner	✔	

Hovedaktørene

Består av de regionale helseforetakene (RHFene), Norsk Helsenett, HDO, Folkehelseinstituttet og Pasientreiser (Sykehusinnkjøp regnes som en hovedaktør, men besvarte ikke spørreskjemaet i sin helhet)

Helse Sør-Øst

Innledning

Helse Sør-Øst mener at for å svare utfordringsbilde vedrørende hvilke tjenesteområder som kan overlates til underdatabehandler (privat leverandør), er det sentralt om tjenesten omfatter personopplysninger, inkludert avidentifiserte, eller om tjenesten kun omfatter anonyme data. Dette må sees i

2 Sykehusinnkjøp fikk ikke tilsendt spørsmålene vedrørende hvilke tjenester som ikke bør settes ut.

forhold til om tjenesten leveres fra Norge, EU/EØS, tredjeland med avtale og tredjeland. Disse utfordrings- og mulighetsbilder presenteres i det følgende i to oversiktsbilder utarbeidet av Sykehuspartner[3].

Offshoring personal data

- PDA chapter V regulates data processing outside Norway. This is in compliance with EU regulation 95/46/EC

From where can the infrastructure be operated?	Norway	The EU and EEA	Third country compliant with 95/46/EC	Third country
Aggregated or anonymous Data*	VERY LIKELY	VERY LIKELY	VERY LIKELY	VERY LIKELY
Personal Data (incl. de-identified data)	VERY LIKELY	PROBABLE	POSSIBLE	NOT LIKELY

High Likelihood of passing a risk assessment *Low*

*Please note that if Personal Data is used as the data source before a data anonymization process, there are *strong requirements* to ensure that data is not backward identifiable towards an individual. Simply removing or changing directly identifiable data such as names or address is not sufficient!

Figur 1: Bruk av databehandler for personopplysninger og anonyme opplysninger

Figur 1 viser utfordringsbildet med bruk av databehandler for personopplysninger, som omfatter også avidentifiserte (indirekte identifiserbare) opplysninger, samt reelt anonyme opplysninger. For tjenester som kun omfatter reelt anonyme opplysninger, er ikke outsourcing i samme grad lovregulert. Det gir dermed en indikasjon på mulighetsrommet.

Examples of operations activities and from where it may be

Examples of operator activities	Norway	The EU and EEA	Third country compliant with 95/46/EC	Third country
Application packaging	VERY LIKELY	LIKELY	PROBABLE	POSSIBLE
ePHI database administration	PROBABLE	POSSIBLE	DIFFICULT	NOT LIKELY
IPT switchboard operations	VERY LIKELY	PROBABLE	POSSIBLE	DIFFICULT
Network Operations Center	VERY LIKELY	PROBABLE	POSSIBLE	DIFFICULT
Data center maintenance and operations	VERY LIKELY	PROBABLE	POSSIBLE	NOT LIKELY

High Likelihood of passing a risk assessment *Low*

Figur 2: Databehandling av personopplysninger fra ulike land

3 Figur 1 og 2 er utarbeidet av Sykehuspartner.

Figur 2 gir et skjematisk bilde over utfordringsbildet ved databehandling (outsourcing) fra ulike landområder.

Målet er effektive, forutsigbare og sikre tjenester innenfor helsesektoren. Bruk av private leverandører vurderes i forhold til lovverk, forskrifter og forordninger samt normer. Innføring av personvernsforordningen (GDPR) skal sikre et felles regelverk i hele Europa. Helse Sør-Øst anser det som meget viktig at det skjer en harmonisering av praksis på dette området, både innenlands og i Europa, slik at det blir enklere å sikre at leverandører leverer på de krav som er gjeldende for Norge.

Helse Sør-Øst har innenfor denne problemstillingen skilt mellom det som er tjeneste- og pasientnært og det som er mer generisk drift av datasystemer (altså ikke så spesifikt for helsesektoren). Det sentrale bør være at det leveres effektive tjenester med rett kvalitet, i tråd med alle krav (lover, forskrifter osv.).

Svar for hvert enkelt tjenesteområde er angitt nedenfor.

Svar vedrørende basisdrift

Med bakgrunn i de erfaringer vi så langt har gjort knyttet til å sette ut basisdrift pågår det en intern prosess knyttet til svar på spørsmålsstilling 1, som vi derfor per i dag ikke kan svare på.

Svar vedrørende applikasjonsdrift og -forvaltning

Applikasjonsdrift og -forvaltning er (for pasientrettede systemer) drifts- og forvaltningsoppgaver som ligger tett opp mot våre kjerneoppgaver som leverandør av helsetjenester, og som derfor i stor grad utføres av Sykehuspartner. De systemene vi bruker er imidlertid i all hovedsak levert av private leverandører, og disse private leverandørene leverer feilrettinger, oppgraderinger osv. og samarbeider med oss i driftssettingen av disse, for eksempel som tredjelinjesupport e.l. Det er derfor behov for betydelig bistand fra private leverandører og deres underleverandører, som også medfører at leverandørene får tilganger til personopplysninger og sensitive person-opplysninger når dette er godkjent av databehandlingsansvarlig i risiko-vurdering og databehandleravtale er inngått. Det planlegges ikke endringer i denne organiseringen av arbeide.

Videre ser vi at det innenfor e-helsetjenester og ikke minst velferdsteknologi skjer en utvikling der private leverandører i økende grad tilbyr tjenester de selv driver, og denne utviklingen kan medføre at vi i økende grad vil måtte forholde oss til privat drift også innenfor dette området (Dette er kommentert ytterligere i andre deler av Helse Sør-Øst svar).

Svar vedrørende applikasjonsutvikling og -innføring

Helse Sør-Øst er lite involvert i leverandørenes utvikling (annet enn ev. som bestiller), men innføring foregår i nært samarbeid med private leverandører. Leverandørene av både de systemene som erstattes og de nye vi setter i drift er stort sett private. Disse leverandørene utvikler altså stort sett selv sine løsninger, stort sett uten at de er i kontakt med våre systemer, mens driftssetting inklusive migrering etc. skjer i tett samarbeid med dem, eventuelt også med den leverandør som har levert det systemet som erstattes. Det planlegges ikke endringer i denne organiseringen av arbeidet.

Oppsummering

Det ligger uansett som en forutsetning for både basisdrift, applikasjonsdrift, applikasjonsforvaltning og applikasjonsutvikling at kontrollen over disse oppgavene alltid må være underlagt og gjenværende i virksomheten. Ved bruk av underleverandører øker virksomhetens kontrollspenn, noe som medfører behov for styrking av egen og underleverandørers internkontroll og kontraktsstyring. Ansvaret endres ikke, og det er risikovurderinger som er det nødvendige verktøyet for å dokumentere tilfredsstillende informasjonssikkerhet og personopplysningsvern hos leverandører og deres underleverandører.

Helse Vest

Innledning

Helse Vest har ikke sett seg nødt til å sette restriksjoner knyttet til enkelte land og jurisdiksjoner i forbindelse med tjenesteutsetting. Det er ikke dermed sagt at vi vil akseptere en driftsmodell hvor et «hvilket som helst» land brukes, men dette vurderes fra sak til sak. Det er i mange henseende forenklende om data ved tjenesteutsetting kan residere i Norge, alternativt innen EU/EØS-områdets indre marked.

Svar vedrørende basisdrift

Helse Vest har så langt ut i fra en samlet vurdering av kost og kvalitet valgt å *ikke* sette ut basisdrift. Dersom basisdrift skulle bli satt ut vil sentrale sikkerhetsfunksjoner ikke bli satt ut. Dette vil for eksempel være brannmurdrift, overvåkning av infrastruktur, sikkerhets og –sårbarhetsovervåkning av servermiljø.

Svar vedrørende applikasjonsdrift

Helse Vest viser til at når det gjelder drift i miljøer utenfor egne (Checkware og Webcruiter) utgjør dette under 1% av totale basisdrift kostnader (BO), nærmere bestemt 0,7%. Helse Vest IKT sin «policy» er i hovedregel å forestå drift i egen regi, og i egne lokaler. Samtidig er det åpning for andre driftsmodeller i anbudsprosesser. Når det kommer løsningsforslag og besvarelser med større eller mindre innslag av tjenesteutsetting vurderes dette fra case til case.

Svar vedrørende applikasjonsforvaltning

Svaret er at vi ikke har noen ekskluderende policy på enkeltland og jurisdiksjoner – men vi har knyttet vår vurdering til hvilken type tjeneste vi ikke ønsker satt ut (sentrale sikkerhetsfunksjoner) – til noen som helst jurisdiksjoner.

Svar vedrørende applikasjonsutvikling (migrasjon, test, driftssetting):

Svaret er at vi ikke har noen ekskluderende policy på enkeltland og jurisdiksjoner – men vi har knyttet vår vurdering til hvilken type tjeneste vi ikke ønsker satt ut (sentrale sikkerhetsfunksjoner) – til noen som helst jurisdiksjoner.
Sikkerhetstesting har vi så langt kun fått gjennomført av norske virksomheter, eller internasjonale virksomheters norske avdeling.

Andre kommentarer

Gjennomgang gjort av Gartner rundt sourcing i Helse Vest viser at vi har en god kostprofil og kvalitetsprofil på dagens drift. Dermed har det vært få drivere for ytterligere sourcing. Det er derfor en noe krevende øvelse å skulle redegjøre for policy knyttet til begrensinger i tjenesteutsetting, både knyttet til tjeneste-områder og hvilke land dette eventuelt skal gjøres fra all den tid vi i svært liten grad benytter tredjepart til full tjenesteutsetting. Med våre tilgjengelige ressurser har vi i begrenset grad evne og anledning til å lage policier og retningslinjer for problemstillinger som i liten grad har vært relevante og etterspurte.

Helse Midt

Innledning

Vi har en leverandørstrategi som omhandler dette med følgende prinsipper:

- Alle virksomhetsnære tjenester skal leveres i egen regi
- Leverandørmarkedet skal brukes for standardtjenester ut fra en vurdering om kostnadseffektivitet og kvalitet.
- Ved skifte i porteføljen for administrative applikasjoner skal ulike leveranse-modeller være en del av vurderingen

Leverandørstrategien er under revidering, ferdigstilles høsten 2017.

Svar for hvert enkelte tjenesteområde er angitt nedenfor.

Svar vedrørende basisdrift

Helse Midt-Norge har som praksis at basisdrift og datalagring foregår i egne datasentre, men kan vurderes ut fra informasjonssikkerhet, kvalitet og kost.

Svar vedrørende applikasjonsdrift

Helse Midt-Norge har den daglige driften av applikasjonen og benytter leverandørmarkedet for feilretting i applikasjonen der dette ikke kan gjøres i egen regi.

Svar vedrørende applikasjonsforvaltning

Helse Midt-Norge bruker i hovedsak leverandørmarkedet. Videreutvikling av applikasjoner gjøres av leverandører på bestilling av Helse Midt-Norge, eller i form av egenutvikling hos leverandøren (nye versjoner). Helse Midt-Norge står for innføring og produksjonssetting, f.eks. håndtering av integrasjoner.

Svar vedrørende applikasjonsutvikling (migrasjon, test, driftssetting)

Helse Midt-Norge bruker i hovedsak leverandørmarkedet ved anskaffelse av nye applikasjoner. Helse Midt-Norge står for innføring og produksjonssetting, f.eks. håndtering av integrasjoner, bruk av leverandørmarkedet vurderes i hvert enkelt tilfelle.

Helse Nord

Innledning

En generell tilbakemelding fra Helse Nord er at outsourcing av drifts- og system-utviklingsoppgaver til leverandører som befinner seg i andre land og på andre kontinent reiser en rekke sikkerhets- og beredskapsutfordringer. Dette gjelder spesielt utenfor EU/EØS. Lokale driftsforhold og nasjonale regler og praksis på området kan avvike fra norske krav til sikker IT-drift eller regelverk knyttet til behandling av helse- og personopplysninger. Nasjonalt tilsyn og mulighetene til å føre kontroll med hvordan den utkontrakterte virksomheten håndterer data kan bli svekket. For å sikre best mulig kontroll må alle anskaffelser vurdere om det vil være forsvarlig å bruke utenlandske tjenesteleverandører i det konkrete tilfellet.

Svar vedrørende basisdrift

Helse Nord har ikke satt ut basisdrift i dag, og det foreligger ingen planer om å vurdere utsetting av hele eller deler av basisdriften.

Svar vedrørende applikasjonsdrift

Helse Nord har i liten grad satt ut applikasjonsdrift i dag, og det foreligger ingen planer om å vurdere ytterligere utsetting av hele eller deler av applikasjonsdriften.

Svar vedrørende applikasjonsforvaltning og -utvikling

Se den generelle kommentaren i innledningen over, i tillegg kan organisering av leverandører utenfor EØS/ EU, og som ikke er på listen over land som er godkjent av Europakommisjonen til å ha forsvarlig databehandling påvirke leveranser. Det vil blant annet være en utfordring rundt support, tilgjengelighet på personell med nødvendig sikkerhetsklarering og riktig kompetanse.

Folkehelseinstituttet

Instituttet behandler i stor grad sensitiv personinformasjon via de forskrifts-baserte helseregistrene, samtykkebaserte helseundersøkelser, laboratorietester (for eksempel ved smittesporing), samt Giftinformasjonen og i varierende grad i forskningsprosjekt.

Folkehelseinstituttet mener basisdrift ikke bør settes ut til private aktører. Da de har basisdrift via NHN er det kritisk for dem at all bruk av underleverandører skal skje etter avtale med Folkehelseinstituttet. Som driftspartner har NHN tilgang til all sensitiv informasjon ved instituttet.

Deres holdning er at utsetting av det dere kaller applikasjonsdrift/forvaltning/ utvikling er avhengig av type system og prosesser disse skal støtte.

Norsk Helsenett

Med mindre det er lovkrav knyttet til dette mener Norsk Helsenett at det kan benyttes private aktører der det er formålstjenlig. Det er viktig framover at leverandørene kan forpliktes på nasjonale lover eller bransjenormer eller lover utarbeidet av EU (GDPR).

Pasientreiser

Pasientreiser HF informerer om at de ikke har gjort en generell vurdering av dette. Drift gjennomføres i dag av Norsk Helsenett.

HDO

HDO har ingen kommentar.

INNSPILL FRA KOMPETANSEMILJØENE

Kompetansemiljøene ble også stilt spørsmålet om det er tjenester som ikke bør overlates til private underleverandører. Det ble mottatt skriftlige svar fra DIFI, Nasjonal sikkerhetsmyndighet og Datatilsynet.

DIFI

DIFI har delvis svart spørsmålet, det vil si de har svart på det som handler om jurisdiksjon.

I henhold til anskaffelsesregelverket er det i utgangspunktet liten mulighet til å skille mellom norske leverandører og leverandører fra EU/EØS-området. Unntaket er «rikets sikkerhet» – i praksis betyr det informasjon og systemer hvor sikkerhetsloven kommer til anvendelse. Det har vært gjort en vurdering av dette spørsmålet i forbindelse med et «Sikker sky»-prosjekt i regi av Nasjonal sikkerhetsmyndighet. Denne vurderingen kan muligens gjenbrukes av Direktoratet for e-helse i arbeidet med dette oppdraget.

Nasjonal sikkerhetsmyndighet

Generelt om tjenesteutsetting av IKT tjenester har NSM følgende råd:

- Tjenesteutsetting av IKT-tjenester til profesjonelle aktører vil kunne gi bedre sikkerhet og mer stabile og tilgjengelige tjenester, lavere og mer forutsigbare kostnader og i større grad bidra til bedre fokus om virksomhetens kjerneaktivitet.
- Tjenesteutsetting medføre Forholdet til sikkerhetsloven er også omhandlet i kapittel 2.1.r økt sikkerhetsrisiko på grunn av redusert kontroll på stadig mer komplekse verdikjeder. Virksomheter må aktivt etablere organisatoriske, prosessuelle, tekniske og juridiske sikringstiltak
- Tjenesteutsetting krever gode risikovurderinger og høy bestiller kompetanse
- NSM er bekymret for at konsolidering av store mengder nasjonale data ikke gjennomføres med nødvendig verdi- og risikovurdering.

En risikovurdering med hensyn på sikring bør bygge på en verdivurdering, en trusselvurdering og en sårbarhetsvurdering. Sammenstillingen av disse bestemmer risikobildet. Verdivurderingen skal identifisere hvilke verdier som er de viktigste for virksomhetens oppdrag og leveranser, konsekvenser ved tap, avhengigheter med mer. Spørsmål om kritikalitet hører hjemme her. Dette er nærmere beskrevet i NSM Håndbok Risikovurdering for sikring.

INNSPILL FRA FAG- OG PASIENTORGANISASJONER

Fag- og pasientorganisasjonene fikk spørsmål om det er tjenester som ikke bør overlates til private underleverandører, og hvilke kriterier legger en til grunn for denne anbefalingen. Vi fikk skriftlige svar på dette spørsmålet fra følgende foreninger: Fagforbundet, NITO, Tekna og Den norske Legeforening. For å lese de tilsendte innspillene fra alle fag- og pasientorganisasjonene, se vedlegg 9. Nedenfor er det en oppsummering av svarene.

Fagforbundet

Fagforbundet mener at IKT-infrastruktur i helse- og omsorgsektoren ikke bør settes ut til private underleverandører. Med IKT-infrastruktur menes her det som muliggjør flyt av elektronisk informasjon i helseforetakene, samt steder hvor denne informasjon lagres. Dette inkludere komponenter som, servere, rutere, switcher, kabler og wifi-nettverk. Slike komponenter bør driftes av IKT-ansatte i helsefortekene. Argumentene for standpunktet om offentlige drevet IKT-infrastruktur er flere. De kan deles i tre underkategorier: Sikkerhet og integritet, kompetanse og samfunnsansvar, samt effektivitetsgevinst.

Fagforbundet mener også at IKT-infrastruktur i helsevesenet bør omfattes av sikkerhetslovens regler om håndtering av samfunnskritisk informasjon.

NITO

NITO mener at drift av IKT-infrastrukturen i dag er for sårbar til å settes ut til private underleverandører. Når det gjelder sikkerhetsloven mener NITOs at i de tilfeller hvor det er sammenfall mellom nasjonal eller regional helseberedskap og IKT-systemer, bør det vurderes å klassifisere IKT-systemene etter bestemmelsene om objektsikkerhet. Dette kan også gjelde større datasentre.

NITO mener tjenester ikke bør overlates til private underleverandører dersom det går utover behovet for å skjerme store mengder helseopplysninger eller at det går utover nasjonal beredskap og helseberedskap. Ved bruk av eksterne leverandører mister man kontroll over driften og bruk av underleverandører kan medføre ansvarspulverisering.

Tekna

Tekna viser til Lysne-utvalgets NOU[4] hvor man trekker frem at utkontraktering til et annet land kan representere en økt sårbarhet i seg selv. Her bør nasjonale myndigheter stille tydelige krav til overordnede sikkerhetsvurderingene.

Tekna mener at drift av systemer med sensitiv pasientinformasjon, som faller innenfor definisjonen av kritisk infrastruktur og som ligger innenfor sikkerhets-lovens virkeområde, skal gjøres i Norge. Nærhet er viktig for slike driftsoppgaver.

4 NOU 2015 Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden

Tekna tar ikke stilling til hvor data lagres, utover at selskapet og personalet som drifter løsningen må være lokalisert i Norge, og underlagt Norsk lov og regelverk. Ved en eventuell lagring av data i et annet land, må risiko og sikkerhetsvurderingen også omfatte en vurdering av lovverk og sikkerhetssituasjon i landet der dataene lagres. Svært sensitive persondata mener Tekna bør lagres i Norge.

Rammene for hva som faller innenfor kritisk infrastruktur må klargjøres av nasjonale myndigheter. Ny sikkerhetslov, som nå er til behandling i Stortinget, vil bidra her, når arbeidet med tilhørende forskrifter og retningslinjer er ferdigstilt. Når man bruker og behandler pasientinformasjon er det avgjørende å sikre integritet, konfidensialitet og tilgjengelighet. Tekna mener derfor det må utarbeides klare nasjonale retningslinjer for innholdet i og gjennomføringen av sikkerhets- og sårbarhetsvurderingene. Dette for å sikre at alle forhold systematisk blir gjennomgått og belyst før virksomheter fatter beslutninger om drift og lagring av data.

Den norske legeforening

Helsetjenesten sysselsetter omtrentlig 300.000 personer, og kanskje 4–5000 jobber spesifikt med IKT på nasjonalt nivå. Med et så stort antall ansatte bør man forvente at nasjonen kan eie og utvikle fagmiljøer innen alle sider av IKT, som er høykompetente. Det er vanskelig å forstå at vi ikke skal kunne drifte våre egne løsninger innenfor landets grenser, og skaper tillitsutfordringer når det blir kjent at sparebehov fører til utflagging av helsedata. Det handler ikke bare om faktisk, men opplevd risiko for den enkelte borger. At IKT i helsetjenesten også er samfunnskritisk infrastruktur betyr også at nasjonen må ha nok kompetanse til å håndtere ulike typer hendelser og ondsinnede angrep på denne infrastrukturen.

INNSPILL FRA IKT-NÆRINGEN

IKT-næringen fikk stilt spørsmålet om det er noen tjenester som ikke bør settes ut til private leverandører og om det bør det skilles mellom ulike jurisdiksjoner (Norge, EØS, globale).

De bedriftene som har svart på skriftlig på dette spørsmålet er IKT Norge, DXC, IBM og Sopra Steria. Nedenfor er det en oppsummering av svarene.

IKT-Norge

Tidsrammen for denne utredningen er altfor smale til å komme med endelig svar, dette må være starten på en prosess som dekket innspill til hvordan outsourcing kan gjennomføres på en god måte og det er flere hensyn som må ivaretas.

IKT-Norge mener det er viktig å fokusere på at outsourcing fungerer bra i tilfellene:

- Der det ikke er tilgang på nok kompetanse i Norge.
- Der det ikke er tilgang på nødvendig spisskompetanse i Norge.
- Der det er høy grad av standardisert og/eller automatisert drift.
- Der det er kritisk å klare å konkurrere på pris for å vinne anbud.
- Der lovverk, f.eks. Sikkerhetsloven, ekomloven, etc., ikke krever at dataene behandles i Norge.

I tillegg mener IKT-Norge at:

- Outsourcing/offshoring kan kvalitetssikres gjennom tydelig regulering, avtaler og prosedyrer.
- Gjøres outsourcing/offshoring på riktig og sikker måte, vil det støtte digitaliseringen i Norge og styrke norske it-selskaper.
- Det er avgjørende at det er bred tillit i prosesser som innebærer outsourcing/offshoring, særlig når det gjelder samfunnskritiske systemer eller opplysninger. Det er derfor viktig med debatt, åpenhet, transparens og spørsmål. IKT-Norge bør bidra til det, og ha full forståelse for andre meninger.

Det er svært viktig at vi i Norge for helsesektoren, som på andre områder, får tydelig retningslinjer. To områder peker seg ut til være basert på en politisk avgjørelse:

- Skal data knyttet opp til helse lagres på norsk jord? I så fall må det avklares hvilke data dette omfattes.
- Skal data knyttet opp til helse behandles av personer som er under norsk lov, har norsk nasjonalitet og/eller jobber i Norge.

DXC

Overall, DXC does not believe there are healthcare systems that cannot be sourced and hosted by private vendors within the healthcare environment

provided the correct controls are in place and the appropriate risk assessments undertaken. DXC is also of the view that the full use of hybrid workload placement (Traditional on premise, Private Cloud and Public Cloud) should be utilized both within and outside of Norway in order to provide access to clinicians and citizens to the best possible healthcare outcomes, whilst providing public service organizations the access to secure, flexible and cost effective solutions.

IBM

IBM mener at det er litt for kort tid for å gi et kvalifisert svar, men bidrar gjerne til en videre prosess for å vurdere dette nærmere. Sikkerhetsmulighetene og de regulatoriske rammebetingelser vil være sentrale også i denne vurderingen. Leverandørenes bruk av internasjonale løsninger vil generelt gi lavere pris til kundene. Det bør vurderes om det kan skilles mellom Norge, Norden, EU/EØS og andre deler av verden. Sikkerhetsløsningene kan eventuelt være ulike, noe som vil være reflektert i prisen. Helseforetakene bør se på å klart skille mellom systemer som inneholder sensitive personopplysninger (pasientdata) og ikke sensitive personopplysninger. Systemer som ikke inneholder sensitive personopplysninger bør kunne prosessers globalt, men systemer med sensitiv personinformasjon kan eventuelt begrenses til færre jurisdiksjoner (Norge/ Norden/EØS – avhengig av sikkerhetskrav). Dataklassifisering av informasjon, også internt i systemer, bør kunne brukes for å bestemme i hvilken jurisdiksjon dataene kan behandles og hvilken ikke er tillatt.

Sopra Steria

Sopra Sterias svar deles opp i to spørsmål:

A. Er det tjenester som ikke bør settes ut til private leverandører?

Sopra Steria mener svaret er et tydelig «nei». Det er ingen grunn til å tro at det finnes oppgaver i dag som kan bli bedre løst av det offentlige alene. Det er viktig nå å finne bedre måter å samhandle på. Bedre måter å utnytte hverandres komparative fortrinn.

B. Bør det skilles mellom ulike jurisdiksjoner (Norge, EØS, globale)?

Sopra Steria mener Lysne-utvalget (Digitalt sårbarhetsutvalg, NOU 2005:13) gir en relevant måte å vurdere dette på:

1. Informasjon som bare bør lagres i Norge
   - Eksempel: gradert informasjon (Sikkerhetsloven)

2. Informasjon som kan lagres i utlandet, men som en må kunne ta hjem om det blir særlig behov for det, og på bestemte betingelser
   - Eksempel: sensitive personopplysninger

3. Informasjon som kan lagres i utlandet uten spesielle betingelser
   - Eksempel: virksomhetsintern informasjon, ingen spesielle regulatoriske krav

VEDLEGG 7:
Endringer av krav og rutiner

Innspill fra de regionale helseforetakene med forslag til endringer i krav, løsninger på utfordringer og forbedringer/endringer i rutiner.

Hovedaktørene i sektoren fikk tre spørsmål hvor det oppfordres til å foreslå endringer eller forbedringer. Disse er:

1. Hvilke innspill til endringer i nåværende krav har dere, for å bidra til at denne formen for tjenester skjer på en ansvarlig måte?
2. Hvilke utfordringer er tilstede ved bruk av private leverandører? Hvilke endringer kan være nødvendige for å gjøre det mulig å bruke det private leverandørmarkedet på en sikker og effektiv måte? Relater det gjerne til nye tjenester og leveransemåter.
3. Hvilke forbedringer/endringer i rutiner ser dere som hensiktsmessige for å sikre etterlevelse av krav til informasjonssikkerhet ved bruk av private leverandører?

Øvrige aktører er også stilt spørsmål om hvilke endringer kan være nødvendige for å gjøre det mulig å bruke det private leverandørmarkedet på en sikker og effektiv måte?

Svarene har gitt innspill som omhandles og drøftes flere steder i rapporten. De formelle svarene fra RHFene, på de tre spørsmålene, er gjengitt nedenfor.

Helse Sør-Øst

Hvilke innspill til endringer i nåværende krav har dere, for å bidra til at denne formen for tjenester skjer på en ansvarlig måte?

Svar: Helse Sør-Øst RHF ønsker at det arbeides for en harmonisering av så vel lover og forskrifter som praktisering av disse, dette også sett i relasjon til innføring av personvernforordningen. Entydige krav og praktisering bør på sikt kunne lede frem til en form for sertifisering av løsninger og leverandører innenfor dette området, hvilket i betydelig grad vil lette arbeidet med innføring og drift av disse.

Hvilke utfordringer er tilstede ved bruk av private leverandører? Hvilke endringer kan være nødvendige for å gjøre det mulig å bruke det private leverandørmarkedet på en sikker og effektiv måte? Relater det gjerne til nye tjenester og leveransemåter.

Svar: Ved bruk av private leverandører er det nødvendig å sjekke leverandøren grundig før avtaleinngåelse, inkludert finansiell situasjon, sikkerhetsrutiner

inkludert rutiner for håndtering av pasientinformasjon, og sikring av pasient-informasjon. Videre må det etableres et tett samarbeid med, og oppfølging av, leverandøren under etablering, innføring og drift. Tjenesteutsetting medfører høye krav til internkontroll, revisjonskompetanse og leverandørstyring og vil ofte kreve styrking av intern kompetanse. Videre, der skytjenester tas i bruk må det sikres at dataene håndteres på riktig måte, bl.a. i forhold til lagring, tilgang til og sikring av dataene, slik at disse ikke kommer på avveier.

Hvilke forbedringer/endringer i rutiner ser dere som hensiktsmessige for å sikre etterlevelse av krav til informasjonssikkerhet ved bruk av private leverandører?

Svar: Det brukes store ressurser for å sikre etterlevelse av krav til informasjons-sikkerhet. Ofte krever dette videreutvikling av internasjonale leverandørers løsninger, dette for å sikre at de tilfredsstiller våre krav. Med innføring av GDPR får vi et felles juridisk rammeverk i EU/EØS, og en harmonisering av praksis innenfor EU og EØS, inkludert Norge, vil gjøre det vesentlig enklere for oss å sikre at de krav som gjelder i Norge (og da også resten av dette området) blir oppfylt. Dette vil ikke bare forenkle anskaffelsene, men også fjerne en betydelig risikofaktor knyttet til innføringen av løsningene, og dessuten legge bedre til rette for bruk av de systemer som vi ser komme innenfor e-helse og velferdsteknologi.

Fra Helse Vest

Hvilke innspill til endringer i nåværende krav har dere, for å bidra til at denne formen for tjenester skjer på en ansvarlig måte?

Det er vanskelig å ha kontroll med underleverandørers underleverandører. En standardisert avtalemal for databehandling, gjerne basert på EUs model clauses ville kunne være nyttig. Det er nok vanskelig for norske virksomheter (som er små i den store verden) å komme med egne versjoner av databehandleravtaler ovenfor tredjepart. Dersom det fantes en omforent, anbefalt og mer eller mindre standardisert avtale man kunne ta utgangspunkt i ville dette være forenklende.

Sertifisering av tredjeparter (både mot informasjonssikkerhet og ovenfor diverse skysertifiseringer) vil være godt for å avklare etterlevelse og god kontroll med informasjonssikkerheten.

Hvilke utfordringer er tilstede ved bruk av private leverandører? Hvilke endringer kan være nødvendige for å gjøre det mulig å bruke det private leverandørmarkedet på en sikker og effektiv måte? Relater det gjerne til nye tjenester og leveransemåter.

Det å verifisere etterlevelse av avtale kontroller og tiltak på informasjons-sikkerhet er komplisert ved bruk av private leverandører. Å ivareta kontroll og å revidere tredjepart vil gjerne være krevende.

Vi vurderer å anskaffe bedre produkt for overvåkning av tredjeparts aktiviteter via VPN.

Hvilke forbedringer/endringer i rutiner ser dere som hensiktsmessige for å sikre etterlevelse av krav til informasjonssikkerhet ved bruk av private leverandører?

Svar: Tydelige retningslinjer rundt pasientnære løsninger med innslag av sky.

Det er behov for avklaring av ansvarsforhold der noen leverandører ønsker full tilgang til data i behandlingshjelpemidler hvor leverandøren da har mulighet for å utlevere til helseforetak. Pasienten samler da selv opplysningene på det utstyret pasienten ønsker å benytte og leverandøren må tilrettelegge for utlevering til HF når HF trenger disse dataene. Da blir leverandøren av det medisintekniske utstyret databehandlingsansvarlig. Dette er en uvant situasjon for helseforetakene. Case her er CGM-målere og dialysemaskiner.

Det er ellers en generell betraktning at det er manglende grenseoppgang mellom hva som er velferdsteknologi og hva som er Medisinsk Utstyr (MU) i sektoren. Her er det store gråsoner der kanskje ingen passer på.

Andre punkter:

- Gode databehandleravtaler herunder adekvat kontroll med underleverandørs underleverandører
- Viktig å få fullstendig beskrivelse i starten fra tredjepart og sikre god samhandling med disse
- Hvordan kan vi sjekke FAKTISK etterlevelse av krav/Normen i leveransen?
- Standardavtaler inn mot Normen – herunder tilpasset GDPR (Model clauses har vært nevnt ovenfor).

Fra Helse Midt

Hvilke innspill til endringer i nåværende krav har dere, for å bidra til at denne formen for tjenester skjer på en ansvarlig måte?

Svar: Det ønskes tydeligere retningslinjer nasjonalt for fortolkning av kravene, med hensyn til blant annet

- Hvor er det akseptabelt å lagre data, hvilke kriterier skal ligge til grunn? Hva er mulig med hensyn til anskaffelsesreglementet?
- Hvilke data er det akseptabelt å gi tilgang til?

Hvilke utfordringer er tilstede ved bruk av private leverandører? Hvilke endringer kan være nødvendige for å gjøre det mulig å bruke det private leverandørmarkedet på en sikker og effektiv måte? Relater det gjerne til nye tjenester og leveransemåter.

Svar: Nedenfor er det listet opp en del områder som Helse Midt-Norge mener bør adresseres fremover mht. å bruke det private leverandørmarkedet på en

sikker og effektiv måte. Dette gjelder både på regionalt nivå og på myndighetsnivå (avklaringer/føringer).

- Tilgangssystemer knyttet til MTU.
- Bruk av leverandørspesifikke skytjenester.
- Leverandører går i større grad mot SaaS, krever kapasitet og kompetanse på avtaler og tjenestekjøp
- Omfattende krav for små leverandører.
- For hvilke områder/omfang må sikkerhetsloven tas hensyn til?
- Blir informasjonssikkerhet tilstrekkelig ivaretatt i inngåelse av nye avtaler (gjelder spesielt Sykehusinnkjøp og MTU)?
- Infrastruktur som støtter skytjenester.
- Det er generelt utfordringer knyttet til at leverandørmarkedet ikke har tilstrekkelig kjennskap til nasjonale krav. Anbefalingene er at regelverket harmoniseres i større grad internasjonalt, ny EU-forordning er et skritt i denne retningen.

Hvilke forbedringer/endringer i rutiner ser dere som hensiktsmessige for å sikre etterlevelse av krav til informasjonssikkerhet ved bruk av private leverandører?

Svar: Tydeligere nasjonale malverk som angår informasjonssikkerhet for anbudskonkurranser, kontraktsinngåelse, databehandleravtaler. Tydeligere krav til logging av tilganger, spesielt knyttet til MTU.

Fra Helse Nord

Hvilke innspill til endringer i nåværende krav har dere, for å bidra til at denne formen for tjenester skjer på en ansvarlig måte?

Svar: I dag er det i utgangspunktet ingen rettslige begrensinger for å ta i bruk leverandører som drifter utenfor Norges grenser forutsatt at mottakerlandet sikrer en forsvarlig behandling av helse- og personopplysningene. Som hovedregel kan det sies at alle stater som har gjennomført EUs personverndirektiv på en tilfredsstillende måte, land som Europakommisjonen har godkjent, og enkeltbedrifter i USA som har sluttet seg til avtaleverket Privacy Shield, anses også å ha en forsvarlig behandling av personopplysninger.

Norge er gjennom EØS-avtalen en del av EUs indre marked med fri flyt av varer, kapital, tjenester og personer (herunder selskapsetableringer). Dette er de såkalte fire friheter. Gjennom EØS-avtalen har Norge forpliktet seg til å sørge for at restriksjoner på grenseoverskridende handel og virksomhet fjernes.

Helse Nord mener at det bør uttredes hvilken betydning det kan få dersom en definerer pasientinformasjon til å være «nasjonal kritisk informasjon», slik at dette ikke omfattet av konkurranseregleне i EUs indre marked.

Helse Nord vil også til å se til vurderingene som IKT-sikkerhetsutvalget skal leverer i løpet av høsten. Utvalget skal se på regelverk og organisering innenfor IKT-sikkerhet. Utvalget skal levere sin innstilling innen 1. desember 2018.

Hvilke utfordringer er tilstede ved bruk av private leverandører? Hvilke endringer kan være nødvendige for å gjøre det mulig å bruke det private leverandørmarkedet på en sikker og effektiv måte? Relater det gjerne til nye tjenester og leveransemåter.

Svar: For utfordringer ved bruk av private leverandører se også svar på neste spørsmål om forbedringsområder.

Det er leverandørene som må tilpasse seg kravene (både nasjonale og EU krav) som stilles for databehandling av helse- og personopplysninger.

Hvilke forbedringer/endringer i rutiner ser dere som hensiktsmessige for å sikre etterlevelse av krav til informasjonssikkerhet ved bruk av private leverandører?

Svar: En rutine vil ikke kunne sikre etterlevelse av krav til informasjonssikkerhet ved bruk av private leverandører. Den databehandlingsansvarlige må forsikre seg om å ha reell kontroll med kravene til informasjonssikkerhet, tilgang til opplysningene som lagres og at kravene til innsyn og sletting er oppfylt ved bruk av private leverandører. Risikovurderinger er et viktig verktøy for å fremskaffe en oversikt over ulike scenarioer som kan oppstå, da dette vil variere fra oppdrag til oppdrag.

Det må derfor gjøres en konkret vurdering for det enkelte oppdrag, og i vurderingen bør det blant annet legges vekt på opplysningenes art, behandlingenes formål og varighet. Jo mer sensitiv karakter opplysningene har, jo høyere krav stilles det til sikkerhet hos den konkrete leverandøren. Behandlingens formål må også vurderes i hvert enkelt tilfelle, da enkelte behandlingsformål kan være mer belastende for personvernet enn andre. Behandlingens varighet skal også vektlegges. Dersom behandlingen skal foregå over lengre tid, vil det stilles strengere krav.

VEDLEGG 8:
Vurdering av land og landområder

I dette vedlegget vil svarene fra hovedaktørene i sektoren på spørsmålet om hvorvidt det settes krav til land leverandøren og leverandørens personell kan holde til i. I tillegg vil det fremheves noen eksempler på kriterier som kan anvendes og kilder som kan være nyttige ved vurderinger av risiko for tjenestekjøp fra ulike geografiske områder.

a) Svar på spørsmål om det settes krav til land leverandørene og leverandørenes personell kan holde til i?

Vi har stilt sektoren følgende spørsmål til de regionale helseforetakene (RHFene):

«Hvis dere benytter private leverandører som skal ha tilgang til pasientinformasjon, hvilke jurisdiksjoner (land) krever dere at leverandørene og leverandørenes personell kan holde til i? Angi svaret med tanke på både historiske og pågående prosesser.»

Svarene viser generelt at få har satt generelle restriksjoner til land, men vurderer jurisdiksjoner som en del av risikovurderingen for den enkelte anskaffelse av en tjeneste eller løsning. Noen opplyser hvilken vurdering som konkret er gjort for en aktuell anskaffelse og disse har generelt valgt å legge seg på et restriktivt nivå, med eksempler på begrensninger til primært Norge og EU/EØS.

Helse Sør-Øst

Helse Sør-Øst viser til felles regionale krav til informasjonssikkerhet som skal benyttes ved anskaffelser og kriterier som må vurderes ved risikovurderingen, og svarer videre «Vi har spesifikke krav som må innfris dersom sensitive personopplysninger skal behandles utenfor Norge. For tredjeland innebærer bestemmelsene slik det fremgår i personopplysningsloven en strengere prøving mht. databehandling, og dette er et scenario som i stor grad søkes unngått. I praksis har en betydelig majoritet av leverandørene våre tilholdssted innenfor EU/EØS-området. Tredjeland, og særlig da såkalte sikre tredjeland, kan vurderes gitt at grunnleggende forutsetninger imøtekommes. For alle tilfeller er det risiko- og sårbarhetsvurderinger som er verktøyet for å vurdere om databehandling kan iverksettes og tilganger kan gis.»

Helse Vest

Helse Vest svarer «Vi har ikke per dags dato satt noen begrensninger på i hvilke områder de private leverandørene kan være (ref. follow-the-sun), men vi har satt begrensinger knyttet til hvilke type informasjon som skal kunne være tilgjengelig for tredjepart i andre land.» Svaret suppleres med «Helse Vest har ikke sett seg nødt til å sette restriksjoner knyttet til enkelte land og jurisdiksjoner i forbindelse med tjenesteutsetting. Det er ikke dermed sagt at vi vil akseptere en drifts-modell hvor et «hvilket som helst» land brukes, men dette vurderes fra sak til sak. Det er i mange henseende forenklende om data ved tjenesteutsetting kan residere i Norge, alternativt innen EU/EØS-områdets indre marked.»

Helse Midt

Helse Midt svarer at «Hemit forholder seg til de retningslinjene som finnes nasjonalt og for EU/EØS. (https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/overfore/).»

Helse Nord

Helse Nord svarer at dette er «Avhengig av hvilket land produktet har sin serviceavdeling. Stort sett Norge, i liten grad USA/EØS» og at «Overføring av personopplysninger er regulert i personopplysningsloven kapittel 5. Her er kravene til hvilke vurderinger som skal gjøres for å sikre en forsvarlig behandling beskrevet. Helse Nord etterlever disse bestemmelsene. I tillegg brukes veiledsmateriell fra Norm for informasjonssikkerhet ved behov.»

Øvrige aktører

Det er fra flere påpekt at i henhold til anskaffelsesregelverket er det i utgangspunktet liten mulighet til å skille mellom norske leverandører og leverandører fra EU/EØS-området.

Det har også blitt stilt spørsmål om det bør skilles mellom jurisdiksjoner (Norge, EØS, globalt) til leverandører og deres organisasjoner. Det er en felles faglig oppfatning av at de ulike regulatoriske rammebetingelser må vurderes og dette vil påvirke utfallet av en slik vurdering. Men det er også kommet innspill som viser ulike syn på hvilke krav til jurisdiksjon det bør kreves at leverandørene eller leverandørenes personell kan holde til i.

b) Eksempler på kriterier som kan anvendes og kilder som kan være nyttige ved vurderinger av risiko for tjenestekjøp

Nedenfor fremheves noen eksempler på kriterier som kan anvendes og kilder som kan være nyttige ved vurderinger av risiko for tjenestekjøp fra ulike geografiske områder.

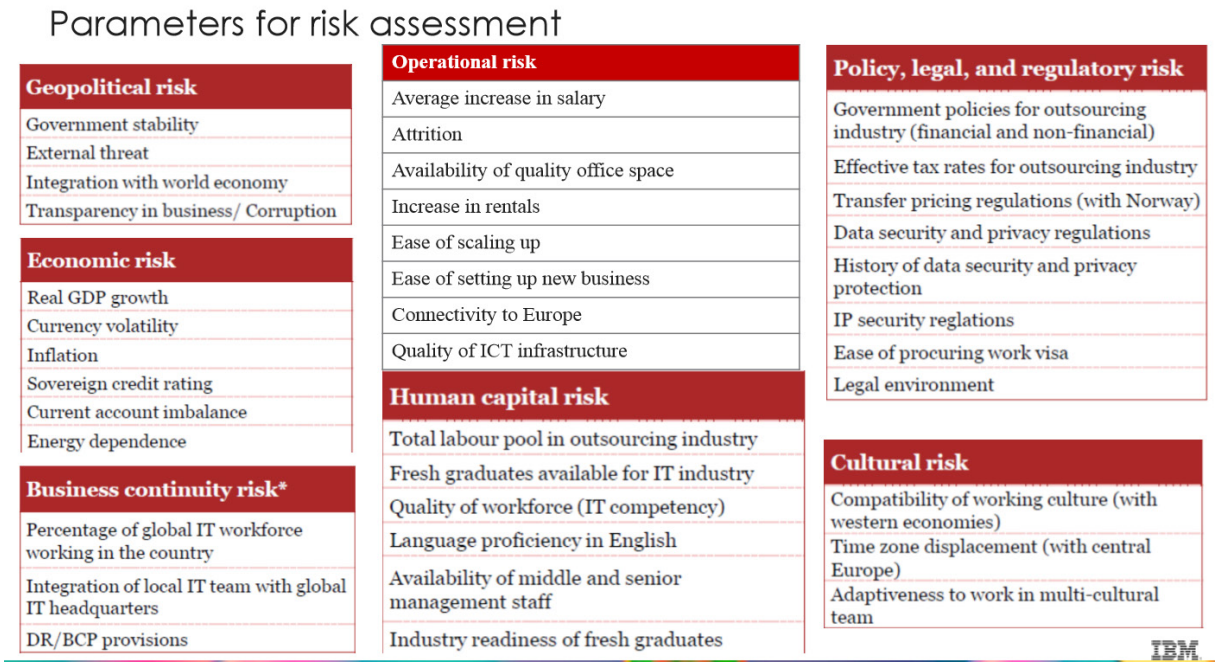
Fra Kredittilsynet har vi fått følgende:
«Når en utkontrakterer IKT-tjenester ut av Norge bør følgende tema om landet det utkontrakteres til, inngå i risikoanalysen:

- Finansiell stabilitet
- Politisk stabilitet
- Levestandard
- Teknisk infrastruktur
- Tilgang på kompetanse – utdanningssystem
- Reguleringer – lover – regler – politi – rettsvesen
- Relevante hendelser i landet»

Fra Kredittilsynet har vi også fått eksempler på flere relevante lenker som kan gi grunnlag for vurdering av land. Blant disse er:

- Transparency Internationals Corruption index, https://www.transparency.org/news/feature/corruption_perceptions_index_2016
- International Monetary Fund, http://www.imf.org/external/pubs/cat/longres.aspx?sk=44318.0
- FATF reporting, https://www.knowyourcountry.com/copy-of-country-reports
- Doing business 2016 – report index at page 5, http://www.doingbusiness.org/rankings
- The Global Ecconomy – political stability country rankings, http://www.theglobaleconomy.com/rankings/wb_political_stability/

Fra IBM har vi fått et eksempel på en liste med mulige kriterierier for vurdering av land, og tillatelse til å gjengi denne:



Direktoratet for e-helse anser også Gartners publikasjon for vurderinger av land og byer, samt deres verktøy for vurderinger som nyttige. Det kreves en lisens for anvendelse av dette materialet, men vi har fått tillatelse til å referere til eksempler på kriterier[5]:

Country Positioning

Cells highlighted in gray are not Gartner ratings

Parameters										
Labor Pool										
Cost										
Educational System										
Infrastructure										
Government Support										
Global and Legal Maturity										
Political and Economic Environment										
Language										
Cultural Compatibility										
Data/IP Security and Privacy										
Overall Average Weighted Rating										

Poor → Fair → Good → Very Good → Excellent

Forhold som et lands kultur for ledelse i næringslivet kan også være relevant for vurdering av risiko ved tjenesteleveranse fra et land. Det eksisterer kartlegginger og analyser hvor enkelte faktorer kan ha betydning for risikovurderingen. Eksempel på kulturanalyse: https://geert-hofstede.com/cultural-dimensions.html

5 Evaluate Offshore/Nearshore Countries for Outsourcing, Shared Services and Captives, 2017.

VEDLEGG 9: Innspill fra fag- og pasientorganisasjoner

I dette vedlegget vil alle skriftlige innspill fra fag- og pasientorganisasjoner presenteres. Følgende aktører sendte sine innspill:

- Fagforbundet
- Den norske legeforening
- NITO
- Norsk sykepleierforbund
- Tekna

Fagforbundet

Invitasjon til å gi innspill – gjennomgang av informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgssektoren

Viser til henvendelse fra Dere datert 29.06.2017 vedrørende gjennomgang av informasjonssikkerhet ved bruk av private underleverandører i helse- og omsorgssektoren. Fagforbundet ønsker å takke Direktoratet for e-helse for muligheten til å gi innspill i denne prosessen. Flere hendelser den siste tiden viser at fokus på kunnskap om IKT og personvern er nødvendig. Det er også et betydelig behov for økt kompetanse om dette på alle ledernivåer i helsetjenesten. Vi setter pris på at utfordringene knyttet til private leverandører tas på alvor og vi imøteser konkrete tiltak på dette området.

Fagforbundet mener at IKT-infrastruktur i helse- og omsorgssektoren ikke bør overlates til private underleverandører.

Med IKT-infrastruktur menes her det som muliggjør flyt av elektronisk informasjon i helseforetakene, samt steder hvor denne informasjonen lagres. Dette inkluderer komponenter slik som, servere, rutere, switcher, kabler og wifi-nettverk. Slike komponenter bør driftes av IKT-ansatte i helseforetakene. Argumentene for standpunktet om offentlig drevet IKT-infrastruktur i helsevesenet er flere. De kan deles inn i tre underkategorier: Sikkerhet og integritet, kompetanse og samfunnsansvar samt effektivitetsgevinst.

Sikkerhet og integritet

Fagforbundet frykter manglende kontroll med tilgang til sensitive person-opplysninger dersom IKT-infrastrukturen utsettes til private aktører. Vi mener erfaringene fra konkurranseutsetting av IKT-infrastruktur i Helse Sør-Øst viser konsekvensene av denne praksisen. Mangelfull styring av tilgang til pasient-opplysninger i helsesektoren har blitt påpekt en rekke ganger. Datatilsynet påpekte mangler i 2008, Riksrevisjonen likeså i 2013. Disse bekymringene ble også uttalt av Utvalget om digitale sårbarheter i 2015. Til tross for dette ser vi

stadige mangler i tilgangskontroller og nødvendige grep må nå tas for å bedre denne situasjonen. Dersom IKT-infrastrukturen blir drevet av helsetjenesten i egen regi, vil dette i betydelig grad bedre kontrollen med tilgang til sensitive helseopplysninger.

Med en økende digital standardisering i helsetjenesten øker også tilgangen til store mengder sensitive helseopplysninger. Flere store prosjekter innen e-helse, slik som prosjektet «Én innbygger – én journal», nødvendiggjør en skjerpet bevissthet når det gjelder sikring av pasientopplysninger. Konsekvensene dersom sensitiv informasjon om pasienter lekker ut, er også meget store. Helsetjenesten er avhengig av tillitt i befolkningen for å kunne besørge sine oppgaver på en adekvat måte. Etterkontroll fra Datatilsynet og logger som sporer aktivitet på serverne kan være nyttig, men de er uten effekt dersom pasientopplysningene allerede er på avveie. Det sentral er å forhindre at datainnbrudd finner sted.

Tjenesteutsetting til private underleverandører medfører også at helsemyndighetene er avhengig av eksterne aktører med andre motiver enn helsemyndighetene selv. Private underleverandører som er basert i fremmende stater forsterker risikoen for at de private aktørene har andre lojaliteter enn det som følger av kontraktsgrunnlaget. Offentlig drevet infrastruktur er dessuten det alminnelige i alle sektorer i samfunnet og det er også hovedregelen internasjonalt.

Fagforbundet mener også at IKT-infrastruktur i helsevesenet bør omfattes av sikkerhetslovens regler om håndtering av samfunnskritisk informasjon. Dette innebærer at regler om sikkerhetsklarering bør følges når tilganger til sensitive helseopplysninger gis. Lovgivningen som gjelder for sensitive helseopplysninger er dessuten langt strengere i andre land som vi kan sammenligne oss med. I Tyskland har de nylig vedtatt nye bestemmelser IKT-sikkerhetsloven (IT-Sicherheitsgesetz), som i betydelig grad skjerper kravene til helsevesenets behandling av sensitive helseopplysninger.

Kompetanse og samfunnsansvar

Utkontraktering av IKT-infrastruktur i helseforetakene leder bort fra regjerningens egen målsetning om et mer sammenhengende helsevesen, senest uttrykt som overordnet strategi i «Nasjonal e-helsestrategi og mål 2017-2022». Dersom driften av IKT-infrastrukturen utsettes til private aktører får man spredte kompetansemiljøer som er frakoblet hverandre. Det er av stor verdi at IKT-ansatte og klinisk personale har samme arbeidsgiver og kan samarbeide på tvers i virksomhetene. Dette vil sannsynligvis bedre pasientbehandlingen og medføre mindre frustrasjon for de ansatte i arbeidshverdagen.

Dersom IKT-infrastrukturen drives av det offentlige, vil dette også sikre et stort IKT-kompetansemiljø i helsesektoren. Dette vil medføre strategiske fordeler, både med hensyn til utvikling av løsninger tilpasset egne behov, innovasjon og andre fordeler knyttet til utviklingen av en rikholdig IKT-sektor. Dette vil også bidra til offensiv næringsutvikling på IKT-området rent generelt.

Det kan også gi gode synergier med utdanningssektoren, som på sin side må besørge arbeidskraft med et høyt faglig nivå. Viktige og gode forbindelseslinjer mellom universiteter, høgskoler og videregåendeskoler kan knyttes til IKT-miljøene i helseforetakene.

Effektivitetsgevinst

I Norge er vannforsyningen kommunalisert ved formell lov og veisystemet er eid og drevet av det offentlige. Dersom man ønsker å realisere en felles IKT-infrastruktur for helse- og omsorgssektoren, vil dette naturlig ligge under helsemyndighetenes driftsområde. Helse Vest RHF har valgt å drive IKT-infrastruktur i egen regi. Både en rapport fra konsulentselskapet Gartner og helseregionens egne tall, viser mindre kostnader til IKT enn de øvrige helseregionene. Drift i egenregi framstår derfor også som svært kostnads-effektivt i tillegg til de tidligere nevnte gevinster. Det er sannsynligvis liten eller ingen effektivitetsgevinst ved å utsette tjenestene til private. Driftskostnadene er i størst grad avhengig av tilstanden på infrastrukturen. Det er med andre ord investeringene som gjøres i infrastrukturen som er det sentrale, og ikke organisatoriske forhold hos den som leverer driftstjenestene. Dette tilsier at det ikke er rasjonelt for helseforetakene å sette dette ut på anbud. Svikt i tilliten til helsevesenet hos pasienter og brukere kan bli både dyrt og vanskelig å reparere.

Konklusjon

De beste grunner taler derfor for at IKT-infrastruktur i helse- og omsorgssektoren beholdes i egen regi. Sentralt står kontroll med tilgang til helseopplysninger, tillitten til helsetjenesten, behovet for IKT-kompetanse internt i helsetjenesten samt effektivitetsgevinster. I mai 2018 trer Personvernforordningen i kraft. Datatilsynet vil forholde seg til et kontrollregime som i større grad baserer seg på etterkontroll. Da er det viktig at helsesektoren selv tar ansvar for å sikre sensitive helseopplysninger.

Den norske legeforening

Legeforeningens innspill til informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgssektoren

Legeforeningen takker for mulighet til å gi innspill til rapport om informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten.

Direktoratet ber om svar på to spørsmål:

- Hvilke kriterier, betingelser og tiltak anser organisasjonene som nødvendig for å kunne benytte private underleverandører på en trygg og ansvarlig måte?
- Er det tjenester som ikke bør overlates til private underleverandører, og hvilke kriterier legger en til grunn for denne anbefalingen?

Primum non nocere (først, gjør ikke skade).

Legeforeningen vil minne om gamle visdomsordet fra Hippokrates, Primum non nocere (først, gjør ikke skade). Dette er et av mantraene legene jobber etter. Derfor er vi forsiktige. Vi må sikre oss at ny teknologi ikke skader. Felles store journaler utfordrer dette prinsippet, selv om det vil være til fordel for svært mange vil noen oppleve konfidensialitetstap eller helsetap. Legeforeningen mener at grundige risikoanalyser er sentrale når man etablerer IKT-systemer i helsetjenesten.

... they were in the 'trust' business not the information business ...

Sitatet kommer fra England der enkelte mener NHS har hatt for stort fokus på å gi tilgang til data, men ikke å ivareta pasientens konfidensialitet. Da undergraver man pasientens tillit til helsetjenesten. Konfidensialiteten er sentralt i helse-tjenesten. Legene og helsetjenesten er avhengig av tillit til at vi tar vare på personene og informasjonen deres. Ikke at vi skal «hente ut gevinster» på deres bekostning. Tillit kan rives ned på et øyeblikk, og tar år å bygge opp igjen. Vi har ikke råd til å skusle bort tilliten til helsevesenet på dette området.

Hvorfor taushetsplikt?

Taushetsplikten skal først og fremst ivareta det nødvendige tillitsforholdet mellom pasient og behandler. Legen får kjennskap til en rekke opplysninger av sensitiv art, ikke bare om helsemessige forhold, men også om personlige forhold, familieforhold, seksualitet, etc. Dersom pasienten ikke har tillitt til at legen holder disse opplysningene for seg selv, risikerer man at essensiell informasjon ikke blir fortalt til legen, eller at pasienten ikke oppsøker legen.

Likevel – flere motstridende hensyn må avveies: Taushetsplikten er viktig for å ivareta personvernet, å skape tillit mellom pasient og lege, hindre misbruk av informasjon. På den annen side er informasjon om pasienter viktig for å kunne gi forsvarlig behandling, danne grunnlag for læring og forståelse, samt avverge fare, for å kunne føre kontroll med helsetjenesten og med ressursbruken samt i en rekke andre viktige sammenhenger.

På den bakgrunn er det nødvendig at vi har et regelverk og en praksis som balanserer disse viktige hensynene. Lovgiver har valgt et system der taushetsplikten er hovedregel, og at unntak skal ha rettslig grunnlag. Det er da viktig at det finnes unntak for de situasjoner hvor det er strengt nødvendig å utveksle informasjon.

Pasientens helsetjeneste

Bør pasienten styre tilgangene selv? Kanskje vi må tenke nytt der også, og gi pasienter utstrakt rett til full bestemmelse ala, «Pasienter har rett til å reservere seg, men også en rett til å utsette seg for fare». Vi må passe på at denne retten ikke går utover andre. Med det menes at vi må støtte de som ønsker å dele informasjon, men også støtte de som ikke ønsker. Den ene gruppen er ikke viktigere enn den andre.

Et absolutt vanntett nivå av informasjonssikkerhet kan i det hele tatt ikke nåes når deling er blitt imperativet, og et hovedspørsmål er derfor hvorledes pasientene kan myndiggjøres til selv å styre sine tilganger og derved selv ta del i risikovurderinger i forhold til egne helsedata. Dette vil være å ta pasientens helsetjeneste ordentlig på alvor. Og da bør det bli slik, at pasienten selv kan sperre, blokkere eller kanskje til og med slette informasjon fra sin journal.

Bygge kompetanse lokalt

Helsetjenesten sysselsetter omtrentlig 300.000 personer, og kanskje 4-5000 jobber spesifikt med IKT på nasjonalt nivå. Med et så stort antall ansatte bør man forvente at nasjonen kan eie og utvikle fagmiljøer innen alle sider av IKT, som er høykompetente. Det er vanskelig å forstå at vi ikke skal kunne drifte våre egne løsninger innenfor landets grenser, og skaper tillitsutfordringer når det blir kjent at sparebehov fører til utflagging av helsedata. Det handler ikke bare om faktisk, men opplevd risiko for den enkelte borger. At IKT i helsetjenesten også er samfunnskritisk infrastruktur betyr også at nasjonen må ha nok kompetanse til å håndtere ulike typer hendelser og ondsinnede angrep på denne infrastrukturen.

Små virksomheter – store krav

Fastlegene og private spesialister er organisert på en meget kostnadseffektiv måte, med lite administrasjon. Innen informasjonssikkerhet er det mange krav å forholde seg til, og selv om Normen lager gode veiledninger oppleves de allikevel som omfattende for de fleste kontorer. GDRP vil også gi økt risiko for virksomhetene.

Legenes primære oppgave er å hjelpe pasienter. Selv om mange leger etter hvert har fått en del innsikt i bruk av ulike tekniske løsninger som benyttes i den praktiske kliniske hverdagen, er det varierende grad av detaljert kompetanse innenfor IKT og teknisk informasjonssikkerhet. Det er ikke gunstig for noen dersom legene må bruke for mye av sin tid på tekniske arbeidsoppgaver at det går på bekostning av pasientbehandling.

Legeforeninger mener derfor det må ses nærmere på hvordan myndighetene og næringslivet sammen kan hjelpe legekontorene i å velge tilfredsstillende og «riktige» løsninger. I dag får gjerne legene utlevert standardkontrakter fra leverandørene, uten at det nødvendigvis er særlig rom for å forhandle frem særskilte klausuler som stiller strengere krav til leverandørene. F.eks. mht. ansvar for sikkerhet for at produktet de leverer skal fungere på en måte som gjør at brudd på etterlevelse av regler om informasjonssikkerhet m.m. ikke oppstår pga. teknisk eller manuelle svikt fra leverandørens side. Med skytjenester vil dette være et sentralt spørsmål.

Legeforeningen mener man bør se nærmere på mulighetene for en sertifiseringsordning for EPJ, og ev. andre elektroniske løsninger som benyttes/ vil benyttes på legekontor og for drift av disse. Dermed kan virksomhetene enklere vurdere leverandørene opp mot hverandre, uten å besitte den informasjonssikkerhetskompetansen som etterspørres. I tråd med at

personvernforordningen innebærer et større ansvar for databehandlere, ville det i det minste kunne utformes anbefalinger, om ikke offisielle sertifiserings-ordninger.

Hvorfor tjenesteutsetting?

Det er viktig å ha klart for seg formålet med tjenesteutsetting før man setter i gang. Skal man rasjonalisere? Skal man effektivisere? Skal man forenkle? Må man spare penger? E-helseløsninger bør være gjenstand for rasjonell drift, vi trenger stordrift, men man må gjøre meget grundige risikoanalyser på forhånd og man må ha tydelig for seg hva formålet med outsourcing er.

NITO

Bruk av private leverandører i helse- og omsorgssektoren

Viser til invitasjon og takker for muligheten til å gi innspill om informasjons-sikkerhet ved bruk av private leverandører i helse- og omsorgssektoren. NITO, Norges Ingeniør- og Teknologiorganisasjon er Norges største organisasjon for ingeniører og teknologer med ca. 85 000 medlemmer. Omlag 10 000 av disse jobber med IKT, og NITO har et eget IKT-fagutvalg som jobber aktivt med IKT-sikkerhet. Våre medlemmer jobber både i privat og offentlig sektor, og ser problemstillingene som tas opp av direktoratet fra mange sider. Når NITO har et stort engasjement for IKT-sikkerhet er det ikke utelukkende fordi vi er opptatt av norske arbeidsplasser, men fordi vi frykter at helsemyndighetene ikke er tilstrekkelig rustet og forberedt i møtet med et nytt og komplekst fagområde. Stadig større bruk av IKT og skybaserte løsninger krever ny og annen sikkerhetskompetanse.

NITO bes om å adressere to spørsmål. Til spørsmål én om hvordan benytte private underleverandører på en trygg måte, vil vi trekke fram behovet for nasjonale minimumskrav for informasjonssikkerhet, slik beskrevet under. Når det gjelder tjenester som ikke bør overlates til private underleverandører, mener NITO at dette ikke bør gjøres dersom det går utover behovet for å skjerme store mengder helseopplysninger, eller at det går utover nasjonal beredskap og helseberedskap. NITO mener at drift av IKT-infrastrukturen i dag er for sårbar til å settes ut til private underleverandører. Når det gjelder sikkerhetsloven mener NITOs at i de tilfeller hvor det er sammenfall mellom nasjonal eller regional helseberedskap og IKT-systemer, bør det vurderes å klassifisere IKT-systemene etter bestemmelsene om objektsikkerhet. Dette kan også gjelde større datasentre.

IKT må være en del av helseberedskapen

Helsesektoren har et nasjonalt ansvar for helsetilbudet til befolkningen, og for helseberedskapen. IKT er et stadig viktigere element i dette bildet. NITO mener at IKT-systemer i helsesektoren i økende grad er av betydning for den nasjonale og regionale helseberedskap. Dersom IKT unntas fra beredskapstankegangen fremstår det som at man ikke tar beredskapen tilstrekkelig alvorlig.

Helsesektorens forvaltning av informasjon dreier seg videre om konfidensialitet. For eksempel dersom opplysningene skulle finne veien til en avisforside eller benyttes til politisk eller økonomisk utpressing. I tillegg er helseopplysningers integritet livsviktig. Manipulasjon av helseopplysninger vil kunne føre til blant annet feilmedisinering. Økende digitalisering gjør at integriteten i helse-systemene er i ferd med å utgjøre forskjellen på liv og død for den enkelte.

En ny rapport om sikkerhet og sårbarhet utført av Helsedirektoratet understøtter NITOs syn.[6] Den sier at IKT er en innsatsfaktor på linje med vann og strøm og definerer dette som kritisk infrastruktur. Det påpekes også at IKT-trusselbildet endrer seg og inkluderer økt interesse for personopplysninger. Det vises også til manglende forståelse for IKT og informasjonssikkerhet som en del av det totale trusselbildet i helsesektoren, særlig blant ledere.

Mer IKT-kompetanse og involvering av tillitsvalgte

IKT-kompetansen må styrkes i besluttende funksjoner, og det må til en økt forståelse for at IKT-sikkerhet koster. Vi ser ofte eksempler på at outsourcing brukes som et argument for at virksomheter skal få fart på digitaliseringen. Underliggende er det ofte et ønske og tro på å spare penger ved å flytte tjenester til lavkostland. Ledelse med manglende kompetanse som utkontrakterer IKT-virksomhet kan ikke nødvendigvis forvente at alt løser seg. Sikkerhetsutfordringer kommer da gjerne tilbake også i form av ekstra kostnader med å rette opp. HSØ-saken illustrerer at man går for fort fram og outsourcer før man har kontroll i eget hus. NITO mener for øvrig at ved outsourcing eller offshoring skal det være åpenhet mot de tillitsvalgte, og det må informeres om hvilke underleverandører som benyttes i lavkostland, og hvordan disse følges opp og kontrolleres.

Behov for nasjonale tiltak og krav for bruk av private leverandører

HOD ber direktoratet om å foreslå rutiner som sikrer etterlevelse av gjeldende krav. NITO setter spørsmålstegn ved om gjeldene krav er godt nok utformet. NITO mener vesentlige nasjonale rammebetingelsene ikke er på plass. Ut fra dagens rammeverk for informasjonssikkerhet virker oppdragsbeskrivelsen fra HOD for snever.

Etabler et nasjonalt rammeverk for informasjonssikkerhet

NITO mener det er behov for nasjonale sikkerhetskrav som treffer offentlige og private aktører likt, inkludert IKT-tjenestetilbydere og underleverandører. De nasjonale sikkerhetskravene bør ikke baseres på frivillighet, men utformes som minstekrav, med tilhørende kompenserende tiltak og avviksrapportering. Norm for informasjonssikkerhet i helsesektoren benytter seg ikke av slike standardiserte sikkerhetstiltak, men forutsetter i stedet at helseforetakene «finner opp hjulet hver for seg». Standardiserte minimumskrav har store fordeler. På et overordnet nivå medfører det at samtlige medarbeidere følger de

6 «Overordnede risiko- og sårbarhetsvurderinger i helse- og omsorgssektoren», https://helsedirektoratet.no/publikasjoner/overordnede-risiko-og-sarbarhetsvurderinger-for-helse-og-omsorgssektoren

samme sikkerhetskravene, uavhengig av organisatorisk tilhørighet. For sektorens del forenkler det gjenbruk av verktøy, prosedyrer og personell på tvers av virksomheter, samt etablerer et helhetlig og gjennomgående sikkerhetsnivå. Ved at det enkelte foretak slipper å lage «hjemmelagde» sikkerhetskrav og mekanismer kan foretakene bruker mer tid og ressurser på sin kjernevirksomhet.

Helsenorm for informasjonssikkerhet lister opp en rekke krav som den enkelte virksomhet har ansvar for. (Blant annet å utarbeide sikkerhetsstrategi, etablere nivå for akseptabel risiko, gjennomføre risikovurderinger). At den enkelte virksomhetsleder skal gjøre alt dette er for det første litt som at «bukken skal passe havresekken». NITO mener det må oppnevnes konkrete personer som har sikkerhetsansvaret. For det andre mangler det kompetanse på ledernivå til å gjennomføre og prioritere dette. Etter vår erfaring overlater man ikke informasjonssikkerhet til virksomhetsleder selv i sektorer som jobber med sikkerhet hver dag, f.eks. forsvarssektoren.

Hovedmomenter i et nasjonalt rammeverk Det første spørsmålet fra direktoratet for E-helse gjelder «hvilke kriterier, betingelser og tiltak anser organisasjonenes som nødvendig for å kunne benytte private underleverandører på en trygg og ansvarlig måte»? Dette dekkes gjennom å etablere et nasjonalt rammeverk som styrker og standardiserer følgende punkter:

1. Fysisk sikkerhet. Passiv sikring av bygninger, rom og datasentre.
2. Personell. Bakgrunnssjekk av alt nøkkelpersonell.
3. Anskaffelser. Krav om IKT-sikkerhetskompetanse ved anskaffelser, standardiserte minstekrav til IKT-sikkerhet i kontraktene.
4. Teknisk IKT-sikkerhet. Overordnet sikkerhetspolicy, sikker arkitektur/design, sikker konfigurasjon, sikker koding, sikkerhetslogging.
5. Prosesser og styringssystemer. Sikker IKT-drift og -utvikling, hendelses-håndtering og gjenoppretting.
6. Helseberedskap. IKT-understøttelse av kritiske helsetjenester i både fred, krise og krig.

Nærmere om punktene i nasjonalt rammeverk

1. **Fysisk sikkerhet** Det bør etableres minstekrav til sikkerheten i fysiske bygningsmasser der det er sensitivt IKT-utstyr, eller hvor det behandles sensitive opplysninger. Dette innebærer krav til etablering og til nivå på adgangskontroll. Vurder inndeling av datasentre, rack og serverrom etter risikokategori; se punkt om «Intern-inndeling av IKT-komponenter etter risiko» under Teknisk IKT-sikkerhet.

2. **Personell** Det bør etableres minstekrav til bakgrunnssjekking av personell som skal ha spesielt utvidede tilganger. Dette gjelder bl.a. IKT-administratorer, forvaltere av IKT-kryptosystemer og forvaltere av adgangskontrollsystemer. Det betyr at det må være dedikerte personer hos leverandør som får tilgang til aktuelle data.

3. **Anskaffelser** Det må innarbeides solide standardklausuler i kontrakt om IKT-sikkerhet, med henvisninger til både personell, prosesser og teknologi (PPT). Det er en selvfølge at det etableres databehandleravtaler. I denne sammenheng må det stilles forventinger, og man må hensynta GDPR (fra mai 2018). NITO mener kontrakten må sørge for at serverne er fysisk plassert i Norge og at dataeier har rett til revisjoner som ikke er varslet i forkant.

   Det bør også være et krav at kontrakter vurderes av personell med IKT-sikkerhetskompetanse, enten man har dette i den anskaffende virksomheten, eller støtter seg på slik kompetanse i departement eller direktorat. Spesielt viktig er det at man krever «sikker programvare-utvikling» når man kjøper ny eller vedlikeholder gammel programvare. I dette ligger både sikker koding og en forpliktelse om retting av sikkerhetsproblemer i hele applikasjonens levetid.

4. **Teknisk IKT-sikkerhet** Generelt bør man etablere felles retningslinjer for sikkerhetspolicy, sikker arkitektur/design, sikker konfigurasjon, sikker koding og sikkerhetslogging. Det må sikres at det ikke gis tilgang til data og IT-systemer som inneholder beskyttet informasjon. Da må det avklares om man har behov for å lagre de dataene man har, hvordan de lagres osv. Videre må det være dedikerte terminaler hos leverandør, all aktivitet i serverne skal registreres, også lesetilgang. Linjene som benyttes mellom leverandør/dataeier og servere skal være kryptert «på øverste nivå» og dataeier skal ha eierskap til, og styring med, krypteringsnøklene.

Spesielt om fjernaksess Dagens nettverksteknologi tillater kopiering av enorme mengder data på kort tid, selv over en bredbåndsforbindelse i et privat hjem. Man bør derfor ikke basere seg på ubegrenset tilgang på nettverksnivå, men i stedet tilby virtuelle arbeidsflater med svært begrensede muligheter for å kopiere ut (potensielt sensitive) data.

For utenlandske leverandørers tilgang til fjernstyring av medisinsk utstyr og applikasjoner, eksempelvis i forbindelse med vedlikehold eller feilretting, bør aksessen snevres inn til forhåndsgodkjente, korte tidsintervaller med innsnevrede brukerrettigheter. Aller helst bør slik tilgang overvåkes av personell lokalisert i helseforetakets bygningsmasse; i alle fall dersom brukerrettighetene er av et visst omfang. Tidsintervallene for vedlikehold bør autoriseres i samsvar med bruksmønsteret for helseforetakets øvrige aktiviteter – både planlagt og akutt, slik at man unngår forstyrrelser på medisinsk utstyr (og tilhørende IKT-støttefunksjoner) som er i bruk. Ideelt bør helseforetakene få etablert en leverandørportal med virtuelle arbeidsflater, hvor de beskrevne begrensningene er normalen.

Dette tiltaket vil ikke hindre en kompetent hacker å utføre stor skade, men begrenser risikoen for uhell og vandalisering ved ordinært vedlikehold.

Intern-inndeling av IKT-komponenter etter risiko

En viktig forutsetning for å kunne håndtere økt risiko i IKT-systemer, er effektiv filtrering, sikkerhetslogging og hendelseshåndtering. Dette er komplekst i seg selv, men vesentlig enklere i en ryddig IKT-arkitektur. NITO anbefaler derfor en sikkerhetskartlegging med sikte på å identifisere sammenhengene mellom helseforetakenes medisinske funksjoner og IKT-tilknyttet medisinsk utstyr, herunder skadepotensiale for helsepersonell, pasienter og medisinske funksjoner / helsetilbud ved manipulasjon eller bortfall. Kartleggingen bør også omfatte IKT-arkitekturmessige avhengigheter, eksempelvis IKT-støttesystemer og fysiske/virtuelle servere.

Deretter bør man etablere risikonivåer i samsvar med den medisinske aktiviteten utstyret understøtter, både med tanke på tilgjengelighet, integritet og konfidensialitet. Til slutt bør sensitive IKT-komponenter plasseres i dedikerte fysiske og virtuelle nettverkssoner med robust perimeterbeskyttelse, kategorisert etter risikonivå.

Kryptografisk integritetsbeskyttelse av alle helsedata

For å motstå eller detektere manipulasjon av helsedata – antakeligvis den viktigste grunnsteinen i fremtidens helse-IKT, må det etableres kryptografiske løsninger som signerer og verifiserer helsedata på et akseptabelt tillitsnivå. Frem til slik beskyttelse er på plass, kan man i prinsippet ikke vite om det er det siste dataviruset, innsideren hos IKT-driftsleverandøren eller legen som har foreskrevet behandlingen og medisinene i IKT-systemet. En kryptografisk signatur sporer opplysningene til den maskinen som har utført den. NITO mener derfor at helsesektoren må etablere minstekrav til, og IKT-løsning for, elektronisk signering av helsedata i helseforetakene og Nasjonalt Helsenett (objektbasert kryptografisk signering og verifikasjon). Spesielt viktig er maskin-til-maskin (m^2m)-kommunikasjon som i eksempelet med «støttesystem for medisinering».

NITO er kjent med at dagens helseløsninger ikke har slik støtte. Bakgrunnen for å fremme et slikt krav er «høna eller egget»-dilemmaet; uten et backend-system for signaturer kommer det neppe støtte i frontend-systemer.

5. **Prosesser og styringssystemer** Det må etableres sikker IKT-drift og -utvikling, sikker hendelseshåndtering og sikker gjenoppretting. Hendelseshåndtering og gjenoppretting må etableres i harmoni med relevante medisinske funksjoner og generell beredskap i foretaket. Herunder planverk og prosedyrer for eskalering av hendelser, samt ekstern bistand.

Spm 2: Tjenester som ikke bør overlates til underleverandører

NITO mener tjenester ikke bør overlates til private underleverandører dersom det går utover behovet for å skjerme store mengder helseopplysninger eller at det går utover nasjonal beredskap og helseberedskap.

NITO mener derfor at drift av IKT-infrastrukturen i dag er for sårbar til å settes ut til private underleverandører. Man må ha kontroll over driften, og gitt dagens situasjon betyr det at man må ha eget personell som drifter IKT-infrastrukturen. Settes dette ut i dag vil vi ikke vite hva leverandøren gjør.

Outsourcing innebærer ofte offshoring fordi underleverandører må spare kostnader. Bruk av underleverandører kan gi ansvarspulverisering mellom utførende leverandør og dataeier. Det gir lavere kontroll.

Spesielt om sikkerhetsloven

Sikkerhetsloven tar for seg både informasjon og objekter av nasjonal betydning eller med nasjonalt skadepotensiale. Helseopplysninger er per definisjon individuelle, og omfattes derfor normalt ikke av bestemmelsene om skjerming i henhold til sikkerhetsloven. For objekter stiller det seg annerledes:

«Et skjermingsverdig objekt er eiendom, område, bygning, anlegg, transportmiddel eller materiell, som kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, om det blir utsatt for sikkerhets-trusler. Objekter kan være et direkte eller et indirekte mål.»

NITOs syn er at i de tilfeller hvor det er sammenfall mellom nasjonal eller regional helseberedskap og IKT-systemer, bør det vurderes å klassifisere IKT-systemene etter bestemmelsene om objektsikkerhet. I tillegg bør man vurdere datasentre av en viss størrelse når disse understøtter større helseforetak.

Norsk sykepleieforbund

- Pasientenes og befolkningens behov for tillit til at informasjon ikke kommer på avveie.
- **Hovedutfordringen er mangel på kunnskap og kompetanse omkring informasjonssikkerhet og hvordan det skal sikres. Dette gjelder i alle nivåer av virksomheten – både toppledelse og hos fagutøvere. Dette er et arbeidsgiveransvar å fokusere på!**
- Behov for et ekstra fokus på ledere og helsepersonell med bestillerfunksjon.
- Informasjonssikkerhet dreier seg både om konfidensialitet og om tilgjengelighet – en balansegang som må håndteres.
- Etablering av rutiner for tilgangsstyring og logging av tilganger.
- Etablering av gode kulturer for informasjonssikkerhet – forankring hos toppledere.

- Etablering av strukturer for løpende kartlegging og håndtering av risiko-områder knyttet til informasjonssikkerheten.
- Kartlegge og håndtere utfordringene rundt leverandører av proprietære plattformer/løsninger.
- I størst mulig grad redusere risikoen for etablering av private leveranse-monopoler innenfor IKT-området.
- Også fokusere på den kommunale helse- og omsorgstjenesten, blant annet fastlegekontorene. Dette ser vi som en risiko.

Tekna

Innspill til gjennomgang av informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgssektoren

Tekna representerer 73 000 medlemmer med master eller doktorgrad innen teknologi og/eller naturvitenskap og er Akademikernes største organisasjon. Våre medlemmer er representert i offentlig og privat sektor og en stor andel jobber med teknologiutvikling og IT.

1. **Hvilke kriterier, betingelser og tiltak anser organisasjonene som nødvendig for å kunne benytte private underlevererandører på en trygg og ansvarlig måte?**

Direktoratet for e-helse etterlyser kriterier, betingelser og tiltak som er nødvendige for å kunne benytte private underleverandører i helse- og omsorgssektoren.

Vi oppfatter at det her er snakk om kjøp av alt fra helseteknologi, applikasjoner og programvare, driftssystemer og infrastruktur samt drift og utvikling av disse fra private aktører, og avgrenses ikke bare til underleverandører. Vi tolker oppdraget til direktoratet, jfr. tillegg til tildelingsbrev nr 4, å dreie seg om hvordan man kan ivareta informasjonssikkerhet knyttet til behandling av personsensitive helseopplysninger.

Det er et stort mangfold av IT-tjenester som på ulike måter vil måtte håndtere personopplysninger, og det er ikke mulig å gi ett sett av kriterier og betingelser som skal gjelde for alle. Det er heller ikke mulig å gi ett sett av kriterier som skal gjelde alle anskaffelser uavhengig av hva slags produkt eller tjeneste man kjøper.

Som en første vurdering må man avklare om virksomheten vil falle inn under sikkerhetslovens virkeområde. I så fall trer en hel del krav til virksomheten inn. Det er det enkelte sektordepartement som skal avgjøre om underliggende organer faller innenfor eller utenfor lovens virkeområde. Regjeringen har oversendt til Stortinget forslag til ny sikkerhetslov med et utvidet virkeområde. Det er viktig at direktoratet i dette arbeidet går grundig gjennom foreliggende lovforslag og ser om dette vil svare på de utfordringer som kan ligge i

vurderingen av sikkerhetsnivået i helse- og omsorgssektorens IT-virksomhet. Det er mulig å få gjennomslag for eventuelle endringer i forelagte lovforslag i stortingsbehandlingen. Tekna ber om å bli orientert hvis man gjennom arbeidet ser svakheter i det lovforslaget som er forelagt Stortinget i god tid før Stortinget avgir innstilling i saken.

Personopplysninger skal behandles i tråd med personopplysningslovens rammer (konfidensialitet). Disse rammene er i endring med implementering av ny personvernforordning fra mai neste år. Deretter må man sørge for at man kan ivareta sikkerheten knyttet til integritet, at dataene er korrekte og ikke kan manipuleres (integritet). Til slutt er det helt avgjørende for et moderne helsevesen at IT-løsningene til enhver tid fungerer på en slik måte at det er mulig å gi nødvendig helsehjelp (tilgjengelighet). Systemet må være robust mot ytre angrep.

For å ivareta alle disse forhold kreves høy og riktig kompetanse, samt tilstrekkelig kapasitet hos anskaffer. Det gjelder kompetanse knyttet til forståelse av lovverk (personopplysningslov, sikkerhetslov, lov om helsetjenester osv.), god system- og teknologiforståelse samt god innsikt og kunnskap om de leverandører som opererer i markedet. Med andre ord må det være god kompetanse in house før man går ut og gjør en anskaffelse. I tillegg er det avgjørende at man har en god plan for oppfølging, implementering og drift i etterkant. Tekna er opptatt av det sikkerhetsvedlikeholdet som må skje i etterkant av anskaffelsen. Et kontinuerlig fokus på retting, feilsøking og videreutvikling av tjenesten eller produktet etter levering, krever en klar plan for oppfølging. Å pulverisere et eksisterende kompetansemiljø i offentlig virksomhet ved utkontraktering av tjenester, vil kunne svekke det løpende sikkerhetsarbeidet i etterkant.

Det er åpenbart at mange, kanskje særlig mindre aktører som små kommuner, små tilbydere av helse- og omsorgstjenester i offentlig og privat regi som fastleger, tannleger, psykologer, drivere av omsorgsboliger osv., ikke har en fullgod forståelse av sårbarheten i sine digitale løsninger. Slik innsikt og forståelse er nødvendig for å kunne gjøre en nødvendig og god ROS-analyse (risiko- og sårbarhetsvurdering) av en anskaffelse fra privat aktør. Tekna mener departementet må vurdere å innføre en form for kvalifisering av private leverandører og en sertifisering av tjenester og produkter for å sikre at det leveres i tråd med kravene til personopplysninger. Det bør også vurderes å stille krav til særskilt kompetanse hos anskaffer.

Videre mener Tekna at det må utarbeides klare nasjonale retningslinjer for hvordan slike risikovurderinger skal gjøres. Nasjonale sikkerhetsmyndigheter må bistå med veiledning og informasjon som kan sikre kvaliteten i vurderingene. Datatilsynet er også en aktør som har en naturlig rolle i veiledningen av aktører som ikke har tilstrekkelig kompetanse i eget hus.

Tekna er bekymret for at sikkerheten og sårbarheten i teknologien og i IT-løsningene ikke blir bakt inn allerede i designfasen. Sikkerhet må være en integrert del i utviklingen av all ny teknologi og IT-systemer. I den sammenheng kan nevnes at Tekna er særdeles opptatt av at sikkerhet skal være en integrert del av all IKT-utdanning. Tekna mener vi i altfor liten grad har vektlagt sikkerhet på utviklerstadiet.

2. Er det tjenester som ikke bør overlates til private underleverandører, og hvilke kriterier legger en til grunn for denne anbefalingen?

Det må alltid vurderes hvilket sikkerhetsnivå man må ligge på før man gjør avtale om en anskaffelse. Skal man kjøpe IT og eller teknologitjenester fra private norske eller utenlandske selskaper, vil man måtte vurdere om en slik utkontraktering i seg selv, utgjør en økt sikkerhetsutfordring. ROS-analyser av kjøp av tjenester innen det vi kan definere som kritisk nasjonal infrastruktur, må underlegges klare retningslinjer for vurdering av risiko fra nasjonale myndigheter. I så fall vil ROS-analysen måtte avdekke om det er tilstrekkelig trygghet for at man kan kjøpe tjenesten uten at man svekker sikkerheten.

NSM har en klar rådgivende funksjon når det gjelder sikkerhets- og sårbarhetsvurderinger. Ved større anskaffelser innen områder som krever høy grad av sikkerhet, kan man tenke seg at man alltid skal ha konferert NSM. NSM kan da gis myndighet til å beslutte om risikoen er større enn forsvarlig nivå, og dermed pålegge at tjenesten må utføres i egen regi eller i det minste av et ikke-utenlandsk selskap.

Tekna viser til Lysne I-utvalgets NOU[7] hvor man trekker frem at utkontraktering til et annet land kan representere en økt sårbarhet i seg selv. Det påligger derfor et ansvar for virksomhetene å ha kunnskap om den nasjonen og den virksomheten som får oppdraget for å gjøre en fullgod ROS-analyse. Her bør nasjonale myndigheter stille tydelige krav til de overordnede nasjonale sikkerhetsvurderingene.

Tekna mener at drift av systemer med sensitiv pasientinformasjon, som faller innenfor definisjonen av kritisk infrastruktur og som ligger innenfor sikkerhetslovens virkeområde, skal gjøres i Norge. Nærhet er viktig for slike driftsoppgaver. Tekna tar ikke stilling til hvor data lagres, utover at selskapet og personalet som drifter løsningen må være lokalisert i Norge, og underlagt Norsk lov og regelverk. Ved en eventuell lagring av data i et annet land, må risiko og sikkerhetsvurderingen også omfatte en vurdering av lovverk og sikkerhetssituasjon i landet der dataene lagres. Svært sensitive persondata mener Tekna bør lagres i Norge.

7 NOU 2015 Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden

Rammene for hva som faller innenfor kritisk infrastruktur må klargjøres av nasjonale myndigheter. Ny sikkerhetslov, som nå er til behandling i Stortinget, vil bidra her, når arbeidet med tilhørende forskrifter og retningslinjer er ferdigstilt. Når man bruker og behandler pasientinformasjon er det avgjørende å sikre integritet, konfidensialitet og tilgjengelighet. Tekna mener derfor det må utarbeides klare nasjonale retningslinjer for innholdet i og gjennomføringen av sikkerhets- og sårbarhetsvurderingene. Dette for å sikre at alle forhold systematisk blir gjennomgått og belyst før virksomheter fatter beslutninger om drift og lagring av data.

Avslutningsvis ønsker Tekna å trekke frem at de mange diskusjonene og stadig nye mediesaker knyttet til sikkerhet og sårbarhet i digital infrastruktur og teknologiske og digitale løsninger, fordrer sterk vekt på utvikling av en sikkerhetskultur i virksomhetene. Det krever en betydelig innsikt i ledelsen for å forstå de muligheter og begrensninger som ligger i systemene, og ledelsen må prioritere dette arbeidet. Tekna mener helse- og omsorgssektoren står overfor en kraftig vekst i sikkerhets- og sårbarhetsutfordringer, og at den tillit vi har til offentlig helsevesen raskt vil kunne svekkes hvis man ikke har et bevisst forhold til hvordan man skal møte disse utfordringene.

Tekna ser frem til rapporten fra Direktoratet for e-helse ferdigstilles. Tekna ønsker gjerne å se innspillene fra de andre aktørene, enten oversendt direkte til oss, eller som vedlegg til den ferdige rapporten.

VEDLEGG 10: Kriterier

Listen over kriterier er å betrakte som et utgangspunkt for en videre prosess hvor også virksomhetene i helse- og omsorgssektoren bidrar. Listen er således ikke komplett og det må også gjøres tilpassinger for ulike tjenester og avtaler.

En vurderingskolonne for hvert punkt skal tillegges og vil kunne omfatte både ja-/nei-svar og/eller rom for graderinger og merknader.

Ledelse og forankring
• Virksomheten har en helhetlig styringsmodell med klarhet i ansvars- og roller knyttet til informasjonssikkerhet som også dekker bruk av private leverandører.
• Styringsmodellen tar høyde for nye behov og krav som oppstår ved bruk av private leverandører.
• Styringsmodellen dekker leverandørstyring fra anskaffelse til avtalen er avsluttet. Ved bruk av store og internasjonale leverandører stiller dette andre krav til leverandørstyring. Disse har også sine egne styringsmodeller som man må forholde seg til og som må kontraktfestes.
• Virksomhetens styre og ledelse oppdateres jevnlig på status for informasjonssikkerhet og personvern.
• Det er på plass rutiner for hvordan rapportering på saker som gjelder informasjonssikkerhet og personvern skal være tilpasset de ulike nivåene i organisasjonen, inkludert involvering av styret og ledelse. – Rapportering inngår som del av en helhetlig styringsmodell i virksomheten. – Rapportering er slik at den sikrer at risikobildet rundt leveranser fra private leverandører fremkommer på en riktig og forståelig måte.
• Styret og ledelse involveres som hovedregel i tilfeller som gjelder bruk av private leverandører og/eller utkontraktering av et visst omfang.
• Det eksisterer rutiner for hvordan styre og ledelse planmessig skal kunne holde seg oppdatert på utviklingstrekk innenfor informasjonssikkerhet og personvern.

Risikostyring

- Virksomhetens risikostyring omfatter alle faser fra anskaffelse til avtalen er avsluttet, og må startes på et tidlig stadium. Risikovurderinger må revideres og oppdateres ved endringer.

- De som utfører risikovurderingene har riktig kompetanseprofil og har en tydelig eskaleringsvei til ledelsen/styret.

- Risikovurderingene har et mandat/omfang som er dekkende nok.

- Virksomheten har oversikt og dokumentasjon på hvordan de ulike komponentene som inngår i verdikjeden henger sammen – fra egen infrastruktur til underleverandører. Det er forståelse for hvilke deler som vil berøres av de tjenestene som den private leverandøren skal utføre.

- Etter at risikovurderingen er foretatt, foreligger det en formelt godkjent plan for risikohåndtering/risikoaksept og oppfølging av tiltak.

- Resultater fra risikovurderingen, risikohåndteringsplan og plan for oppfølging av tiltak kommuniseres på rett detaljnivå til overordnet ledelse og styret.

- Risikovurderingen er tilpasset tjenesten som leveres og omfatter de momenter som bør besvares, med utgangspunkt i viktige spørsmål:
  - Vil leverandøren kunne få tilgang til pasientinformasjon?
    - Hvilken type pasientinformasjon gjelder det (sensitive/ikke-sensitive opplysninger)
    - Omfang på tilgang og i hvilke situasjoner?
    - Hvordan begrense tilgang til kun de områder som er nødvendig og for angitt formål og tidsperiode?
  - Hvordan er tilgangsstyringen sikret for tidsperioden hvor tilgang må gis?
  - Hvordan er pasientinformasjon sikret (F.eks. kryptering og signering, anonymisering, aggregering og pseudonymisering)?
  - Hvordan kan man spore hva leverandøren har utført og hatt tilgang til? Hvordan oppdage eventuelle avvik (For eksempel logging av tilganger til tekniske løsninger, dataelementer og verktøystøtte for håndtering av hendelser og endringer, samt konfigurasjonsstyring)?
  - Hvor gode er leverandørens interne kontrollrutiner?
  - Hvor komplekst er aktørbildet (løsninger, produkter, aktører, underleverandører, verdikjeder).
  - Jurisdiksjon; hvilke land befinner personer i, som kan komme til å få tilgang til pasientinformasjon eller hvor lagres disse data?
  - Hvordan håndteres driftsavbrudd og kriseberedskap?

Planlegge, vurdere og velge leverandør

- Virksomhetens styringssystem for informasjonssikkerhet inneholder rutiner for håndtering av leverandører. Rutinene er integrert med virksomhetens anskaffelsesprosesser og omfatter klassifisering av informasjon som vil bli delt med leverandør.

- Det sikres at relevante sikkerhetskrav inngår i alle anskaffelser, og at nødvendig kompetanse på sikkerhet og personvern medvirker i kravstilling og evaluering.
- Spørsmål knytte til relevante sikkerhetskrav kan være:
  - Dekkes de behovene som framkommer i risikovurderinger?
  - Dekkes regulatoriske krav og krav som følger av avtaleforpliktelser?
- Er det bestemt hvordan disse skal vektes, og om enkelte sikkerhetskrav skal være obligatoriske?

- Det finnes tilstrekkelig bestillerkompetanse på alle nødvendige områder. Rutiner må være på plass som beskriver hvordan nødvendig bestillerkompetanse er sikret i anskaffelsesprosjekter, herunder hvordan og hvilken kompetanse på sikkerhet og personvern som skal inngå i anskaffelsesprosjektet i forbindelse med kravstilling, evaluering og eventuelt forhandling

Inngå kontrakt, oppstart med leverandør

- Det er kvalitetssikret at kontrakten inneholder nødvendige sikkerhetskrav
- Det er definert hva slags sikkerhetstesting som skal foretas, for eksempel penetrasjonstest for å verifisere at kundens data er sikre.
- Det må være på plass adekvate tekniske tiltak for styring og kontroll av IKT-personells tilgang til pasientinformasjon.
- Det er etablert tydelige, omforente planer for etablering av sikkerhetstiltak på bakgrunn av risikovurderinger som er gjort. Inkludert, dersom tekniske tiltak ikke er gode nok, hvilke andre tiltak er innført for å få akseptabelt risikonivå
- Rutinene i Normens fjernaksessveileder følges.
- Er det behov for og satt krav til beskrivelse av, og eventuelt innsyn i, de interne rutiner og mekanismer som leverandøren har og hvilke sertifiseringer leverandøren har?
- Aktuelle spørsmålsområder for å sikre at kontrakt dekker relevante sikkerhetsforhold:
  - Prosess for etablering av databehandleravtale i de tilfellene dette er relevant.
  - Databehandlingsansvarlig skal på forhånd godkjenne databehandlers eventuelle underleverandører.
  - Behovet for at leverandørens underleverandør oppfyller de samme sikkerhetskravene som stilles til leverandøren.
  - Krav om rapportering og håndtering av sikkerhetshendelser.
  - Retten til å utføre testing og revisjon hos den private leverandøren og dens underleverandører. Frekvens, type revisjon, og ev. bruk av 3. partsrevisjon bør angis.
  - Behovet for sikkerhetsrelatert ytelsesovervåkning og rapportering på fastsatte KPI-er.
  - Muligheten til å reforhandle vilkår og betingelser i kontraktens løpetid (eller ved definerte intervaller) på grunn av endringer i risikonivå.
  - En exitplan og klare vilkår ved avslutning av kontrakten. Dette må omfatte krav om at alle data tilhørende kunden er slettet eller tilbakelevert og rett til en skriftlig erklæring fra leverandøren som bekrefter dette.
  - Rutiner for test, blant annet vurdering av i hvilke tilfeller reelle/produksjonsdata kan benyttes, med tilhørende sikkerhetstiltak.
  - Leverandørene gir til enhver tid gir en komplett oversikt over hvilke enheter innen strukturen (konsernet og underleverandører) som benyttes for å levere tjenester og i hvilket land disse holder til i, samt at det er inngått databehandleravtaler med alle aktører.

Oppfølging og rapportering

- Løpende landvurderinger / globalt trusselbilde håndteres

- Det gjennomføres jevnlige revisjoner av leverandøren etter en fastsatt plan. Viktige forhold skal være beskrevet:
  - Hvordan revisjon av leverandører skal foregå, for eksempel med henvisning til relevante internasjonale standarder.
  - Etablering av revisjonsplan og prosess for endringer av denne.

- Løpende oppfølging av at kontraktens krav til sikkerhet og rapportering oppfylles, og at man foretar nye vurderinger ved endringer av avtalen.

- Eksempler på rutiner:
  - Fjernaksess til løsningene ved feilretting og support
    - Se Normens fjernaksessveileder
  - Innsending av utstyr, for reparasjon eller utfasing
    - Se Normens faktaark 34 – Håndtering av lagringsmedia
  - Oppdatering av lister over underleverandører og avtaler med dem
  - Rapportering og håndtering av sikkerhetshendelser
  - Rutiner ved test, oppgraderinger og revisjoner
  - Håndtering av endring av rutiner og avtaler ved endringer i teknologi, lovverk og risikonivå
  - Systematisk/regelmessig oppfølging av databehandleravtaler mot underdatabehandler (leverandør/underleverandør)
  - Systematisk/regelmessig rapportering på databehandleravtaler overfor databehandlingsansvarlig

- Ved terminering av kontrakten, skal det foreligge en signert erklæring fra leverandøren om at alle data tilhørende virksomheten er tilbakelevert eller slettet til avtalt tid.

- Om bytte av underleverandør er aktuelt, underrettes alltid virksomheten og skal det kreves at virksomheten på forhånd godkjenner ny underleverandør?

- Virksomhetens kontinuitetsplaner bør dekke tilfeller der leverandørens (med underleverandører) tjenester blir utilgjengelige, planlagte eller ikke-planlagt, samt varslings eller godkjenningsprosesser ved endringer i leverandørens eierstrukturer.

Kompetanseheving

- Det foreligger tydelige krav til nødvendig kompetanse innen informasjonssikkerhet og risikovurderinger hos blant annet:
  - Ledelsen og styret
  - De som arbeider med anskaffelsene (bestillerkompetanse)
  - De som arbeider med innføring og oppfølging

- Det må være på plass nødvendige rutiner for kompetansebygging innen informasjonssikkerhet, personvern og risikovurderinger ved kjøp fra private leverandører i et større marked.

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Postadresse
Postboks 6737
St. Olavs plass
0130 OSLO