Personvern og informasjonssikkerhet – medisinsk utstyr

Versjon 2.0
Juni 2021

Utarbeidet med støtte fra Direktoratet for e-helse

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

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

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

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

Innhold

1. Innledning

1.1 Bakgrunn

Produkter og systemer som skal benyttes i medisinsk sammenheng er underlagt bestemmelser som skal ivareta både pasientsikkerhet og personvern/informasjonssikkerhet. Medisinsk utstyr skal også brukes og vedlikeholdes slik at det ikke medfører fare for pasienten/brukeren. Aktuelt lovverk som regulerer området er omtalt i kapittel 2.
Med **«Medisinsk utstyr»** menes i denne veilederen ethvert instrument, apparat, utstyr, programvare, materiale eller annen gjenstand som brukes alene eller i kombinasjon, herunder programvare som av produsenten er tiltenkt å brukes spesielt til diagnostiske og/eller terapeutiske formål og som kreves for riktig bruk, og som er ment å skulle brukes på mennesker med sikte på:

1. diagnostisering, forebygging, overvåkning, behandling eller lindring av sykdom,
2. diagnostisering, kontroll, behandling, lindring eller kompensasjon for skade eller handikap,
3. undersøkelse, utskifting eller endring av anatomien eller av en fysiologisk prosess, eller
4. svangerskapsforebyggelse,

og der den ønskede hovedvirkning i eller på menneskekroppen ikke framkalles ved farmakologisk eller immunologisk virkning eller ved å påvirke stoffskiftet, men der slike effekter kan bidra til dets funksjon.

Medisinsk utstyr (MU) behandler i mange tilfeller helse- og personopplysninger, og er dermed underlagt Normens krav. [1] Normens hovedkrav til medisinsk utstyr som behandler helse- og personopplysninger er at dette skal inkluderes i virksomhetens arbeid med informasjonssikkerhet og personvern, herunder i risikovurderinger, tilgangsstyring og rutiner for bruk, på lik linje med informasjonssystemer.

I vurderingen av sikkerhetstiltak for medisinsk utstyr, vil eventuell påvirkning på funksjon og bruk av utstyret måtte tillegges stor vekt. Kravet i personvernlovgivningen om at sikring skal være forholdsmessig må derfor veie tungt når sikkerhetstiltak for medisinsk utstyr skal implementeres.

Samtidig vil informasjonssikkerhetstiltak ofte også være med å øke pasientsikkerheten, ved at tilgjengelighet og motstandsdyktighet mot digitale angrep bedres.

Oppmerksomheten rundt digitale trusler og medisinsk utstyr er også økende, bl.a. omtalt av amerikanske og europeiske myndigheter.

Det ligger utenfor Normens virkeområde å gi en detaljert beskrivelse av hvordan pasientsikkerhet skal risikovurderes i tilknytning til MU, men det pekes i veilederen på hvordan standarden IEC 80001 kan benyttes for å gjennomføre helhetlige risikovurderinger som kombinerer informasjonssikkerhet og funksjon/bruk.

[1] I denne veilederen benyttes begrepet *medisinsk utstyr* (MU) siden dette er begrepet som benyttes i aktuelle forskrifter (se kapittel 2). I enkelte andre dokumenter utgitt av styringsgruppen for Normen er det tidligere benyttet andre begreper som medisinskteknisk utstyr og elektromedisinsk utstyr.

Medisinsk utstyr kan bestå av maskinvare- og/eller programvarekomponenter som kan være sårbare for digitale angrep. Slikt utstyr er også i økende grad tilknyttet andre nettverk, f.eks. sykehusets lokalnett. Dette øker risikoen for sikkerhetsbrudd. For medisinsk utstyr kan dette være alvorlig, særlig hvis et angrep setter livsnødvendig utstyr ut av spill.

Sikkerhetstiltakene som innføres for å sikre utstyret og informasjonen som behandles skal være effektive mot mange typer trusler. Truslene kan komme fra både interne og eksterne aktører, og true både konfidensialitet, integritet og tilgjengelighet. Det er bl.a. en sterk økning av angrep på digital infrastruktur. Et angrep kan ramme utstyret i seg selv, men utstyret kan også bli et brohode inn mot annen infrastruktur ved f.eks. et virusangrep.

Denne veilederen adresserer særlig to aspekter ved informasjonssikkerhet: manglende evne til å behandle helse- og personopplysninger i tråd med lovverket og dermed true pasientens personvern, og hvordan medisinsk utstyr kan beskyttes mot angrep på digital infrastruktur. En del aktuelle trusselscenarioer/uønskede hendelser til bruk i risikovurdering finnes i vedlegg til denne veilederen, se kapittel 6.2.

En utfordring ved å sikre medisinsk utstyr er at tiltak som normalt brukes for å ivareta informasjonssikkerhet (som f.eks. tilgangsstyring, antivirus og sikkerhetsoppdateringer) griper inn i utstyrets funksjon eller bruk. Funksjonalitet som understøtter informasjonssikkerhet er ofte ikke støttet i utstyret eller av produsenten . Mye medisinsk utstyr og tilhørende programvare er f.eks. ikke tilrettelagt for tilgangsstyring på linje med journalsystemer, og i mange tilfeller vil krav til personlig pålogging ikke være hensiktsmessig for personell som skal benytte utstyret. Videre har produsenten av medisinsk utstyr ansvar for at utstyrer fungerer etter hensikten. Hvis eier (virksomheten) gjør egne modifikasjoner vil dette innebære å påta seg produsentansvaret for utstyret. Dette innebærer at implementering av antivirusprogramvare og sikkerhetsoppdateringer må gjøres i samråd med leverandør. Dette kan medføre en lavere oppdateringstakt enn det som er anbefalt for å sikre seg mot stadig nye digitale trusler.

Når medisinsk utstyr lagrer helse- og personopplysninger er det å anse som et behandlingsrettet helseregister, jf. lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven). Derfor vil vanlige regler om behandling av helse- og personopplysninger i behandlingsrettete helseregistre også gjelde for opplysninger som finnes i slikt utstyr. Det er likevel forskjell på medisinsk utstyr og andre behandlingsrettete helseregistre når det gjelder sletting av opplysninger. Opplysninger i pasientjournal skal som regel ikke slettes, med noen få lovregulerte unntak. Pasientjournalforskriften gjelder alle former for behandling av helseopplysninger som dokumenteres etter helsepersonelloven, også lyd- og bildeopptak.

1.2 Tema for veilederen

Veilederen skal bidra til å skape felles forståelse for krav og tilnærming til informasjonssikkerhet hos virksomheter som benytter medisinsk utstyr, databehandlere/driftsleverandører og leverandører av medisinsk utstyr[2]. Den skal gi

[2] En *leverandør* av *medisinsk utstyr* kan også i en del tilfeller være/inneha rolle som driftsleverandør. For eksempel multimonitorløsninger med overføring av medisinske data fra ambulanser til sykehus.

veiledning til å tolke Normens krav til behandling av helse- og personopplysninger i medisinsk utstyr med tilhørende systemløsninger og applikasjoner på en praktisk måte.

Veilederen omhandler informasjonssikkerhet og personvern for medisinsk utstyr basert på kravene i Normen.

Kapittel 2 gir oversikt over og tydeliggjør enkelte sentrale lovbestemmelser ifm. medisinsk utstyr med tilhørende systemløsninger/applikasjoner og personvern/informasjonssikkerhet

Kapittel 3 gir en del overordnede og grunnleggende krav som må være på plass hos virksomheter som benytter medisinsk utstyr, særlig knyttet til styring og ansvar.

Kapittel 4 inneholder tiltak med veiledning knyttet til informasjonssikkerhet.

Veilederen har som utgangspunkt at utfordringsbildet som beskrives i kapittel 1 må løses gjennom en risikobasert tilnærming. Dette innebærer at første steg for en virksomhet som vil oppnå bedre informasjonssikkerhet for medisinsk utstyr er å ha oversikt over utstyr og systemer i virksomheten, deretter risiko og sårbarheter. Deretter settes tiltak inn der risikoen er størst og nytten av tiltakene gir størst gevinst. Kapittel 5 beskriver nærmere hvordan en risikobasert tilnærming til informasjonssikkerhet og medisinsk utstyr kan følges i virksomheten, samt en del bruksscenarier og egenskaper for medisinsk utstyr med ulike sikkerhetsmessige utfordringer. Det refereres fra disse bruksscenariene og egenskapene til kapittel 4 der tilhørende sikkerhetstiltak og sikkerhetskrav som nevnt omtales nærmere.

1.3 Målgruppe

Målgruppene for veilederen er personell som har ansvar for og/eller oppgaver i forbindelse med medisinsk utstyr, IKT og informasjonssikkerhet.

Aktuelle brukere av denne veilederen kan omfatte:

- Medisinsk teknologisk avdeling (MTA)
- Ansvarlige i virksomheten for håndtering av medisinsk utstyr
    - Helseforetak og private virksomheter
    - Kommune
    - Røntgeninstitutter/laboratorier mv.
    - Tannleger
    - Leger
    - Andre
- Ansvarlige for anskaffelse av utstyr
- Produsent og leverandør
- Driftsleverandør/databehandler
- Informasjonssikkerhetsleder/personvernombud
- «Medical it-network risk manager (se kapittel 5.2.2)
- Behandler/helsepersonell (brukere av medisinsk utstyr)

I tillegg vil veilederen være aktuell for leder med formelt dataansvar i virksomheten.

Veilederen omtaler både produsent og leverandør. *Produsenten* er den som ansvarlig for konstruksjon, framstilling, emballering og merking av et utstyr med sikte på å markedsføre

det i eget navn, uansett om de aktuelle arbeidsoperasjoner utføres av vedkommende selv eller av tredjemann på dennes vegne. Denne definisjonen er i tråd med midlertidig forskrift om medisinsk utstyr, § 1-5 f. *Leverandør* benyttes i veilederen som den som helsevirksomheter som tar i bruk medisinsk utstyr har et kunde-leverandørforhold til, og som typisk bistår med tjenester som fysisk service og fjernaksess. Produsentens forhandlerledd vil i mange tilfeller være leverandør.

1.4 Krav i Normen

I Normens kapittel 5.3.6 heter det at medisinsk utstyr som behandler helse- og personopplysninger, skal inkluderes i virksomhetens arbeid med informasjonssikkerhet og personvern, herunder i risikovurderinger, tilgangsstyring, endringskontroll og rutiner for bruk, på linje med andre informasjonssystemer.

I kapittel 5.5.5 er medisinsk utstyr nevnt som eksempel på teknisk utstyr som kobles til internett, og som dermed i slike tilfeller skal inkluderes i virksomhetens arbeid med informasjonssikkerhet og personvern, herunder i risikovurderinger, tilgangsstyring og rutiner for bruk.

Veilederen omtaler utover dette et bredt utvalg av Normens krav og på hvilken måte disse er relevante i forbindelse med medisinsk utstyr.

1.5 Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk

Regelverk er omtalt i kapittel to i veilederen.

1.6 Avgrensninger

Veilederen dekker medisinsk utstyr som forvaltes av en virksomhet, og ikke slikt utstyr som pasienten/brukeren har anskaffet selv. Sett i lys av utviklingen av helseapper og personlig sensorteknologi er dette et område som det er grunn til å tro vil få økende oppmerksomhet, og der det kan oppstå gråsoner mellom hva som er privat bruk og der virksomheten har et ansvar. Videre vil frittstående medisinsk utstyr der det ikke behandles helseopplysninger ikke omtales av denne veilederen.

1.7 Utvikling av veilederen

Arbeidet med første versjon av veilederen startet i 2014. Utviklingen skjedde i samarbeid med en referansegruppe. Gruppen besto av fagpersoner innen medisinsk teknologi, IKT og sikkerhet fra flere helseforetak. I tillegg deltok representanter fra leverandørsiden og tilsynsmyndigheter.

Fagpersoner innen medisinsk teknologi har gitt innspill i arbeidet fram mot versjon 2.0.

2. Regelverk

I dette kapitlet blir sentrale lovbestemmelser ifm. medisinsk utstyr og personvern/informasjonssikkerhet omtalt. Kapitlet inneholder ikke en uttømmende oversikt over gjeldende lover og regler, men de sentrale bestemmelsene innenfor Normens ansvarsområde.

2.1 Forskrift om håndtering av medisinsk utstyr[3]

Forskriften setter krav til virksomhetenes interne rutiner og kvalitetssystemer for bruk av medisinsk utstyr. Forskriften definerer videre elektromedisinsk utstyr som ethvert medisinsk utstyr, inkludert systemløsninger, som er avhengig av en elektrisk energikilde for å fungere. Det settes blant annet krav til rutiner for anskaffelse, opplæring i utstyret, bruk, vedlikehold og hvordan utstyret skal oppbevares. Den er gjeldende for helsetjenesten og helsepersonell som yter helsehjelp, som sykehus, pleie- og sykehjem, klinikker, legekontorer og tannlegekontorer. Forskriften trådde i kraft 1. januar 2014.

2.2 Lov og forskrift om medisinsk utstyr

Loven og forskriften gjennomfører forordning (EU) 2017/745 om medisinsk utstyr (MDR) og forordning (EU) 2017/746 om in vitrodiagnostisk medisinsk utstyr (IVDR) i norsk rett. Disse er omtalt under. For MDR vil deler av loven og forskriftsutkastene tre i kraft samtidig, dvs. 26. mai 2021. Siden ikrafttredelse er planlagt nær tidspunktet denne veilederen er planlagt publisert, vises det til Statens Legemiddelverk sine nettsider for mer informasjon.

Forordningene om medisinsk utstyr og in vitrodiagnostisk medisinsk utstyr[4] trådte i kraft i EU 26. mai 2017 og Norge har implementert forordningene gjennom ny lov om medisinsk utstyr. Formålet med forordningene er å sikre at medisinsk utstyr er trygt når det plasseres på markedet samtidig som det nye regelverket skal fremme innovasjon av medisinsk utstyr. Det nye regelverket vil styrke pasientsikkerheten og sørge for et enhetlig regelverk i hele EØS-området. For medisinsk utstyr er det en overgangsperiode på tre år.

Det følger en rekke krav til elektroniske programmerbare systemer i forordningen om medisinsk utstyr (utstyr som inneholder programmerbare systemer og programvare som er utstyr i seg selv):

- Utstyret skal designes slik at det sikres at repeterbarhet, pålitelighet og ytelse er i samsvar med den tiltenkte bruken. Ved feil i utstyret, skal det treffes egnede tekniske tiltak slik at risikoene eller den svekkede ytelsen som dette kan innebære, fjernes eller reduseres så langt som mulig.
- Utstyret skal utvikles og framstilles i samsvar med det aktuelle tekniske nivået, idet det tas hensyn til prinsippene for utviklingslivssyklus, risikohåndtering (herunder informasjonssikkerhet, verifisering og validering).

[3] https://lovdata.no/dokument/SF/forskrift/2013-11-29-1373
[4] https://lovdata.no/dokument/NL/lov/2020-05-07-37?q=lov%20om%20medisinsk%20utstyr

- Utstyr som er beregnet på bruk i kombinasjon med mobile databehandlingsplattformer skal utvikles og framstilles slik at det tas høyde for den mobile plattformens særlige egenskaper (f.eks. skjermens størrelse og kontrastforhold), og ytre faktorer knyttet til bruk (skiftende lys- eller støynivå i omgivelsene).
- Produsenter av utstyret skal fastsette minstekrav til maskinvare, IT-nettverkenes egenskaper og IT-sikkerhetstiltak (vern mot uautorisert tilgang, som er nødvendige for å kunne bruke programvaren som beregnet).[5]

Forordningen for medisinsk utstyr (MDR) har på lik linje som personvernforordningen en risikobasert tilnærming. MDR handler hovedsakelig om pasientsikkerhet, men også her må produsenten inkludere informasjonssikkerhet i risikovurderingene, selv når informasjonssikkerheten ikke er direkte nevnt i bestemmelsene. Flere og flere typer medisinsk utstyr kobles til nettverk og gjøres digitale. Basert på dette øker også risikoen for brudd på informasjonssikkerheten og personvernet.

Operatører og brukere som inkluderer helsepersonell og pasient/bruker er ansvarlige for å bruke det medisinske utstyret basert på instruksjonene fra produsenter.

Medical Device Coordination Group (MDCG) har utarbeidet en veileder for cybersikkerhet i medisinsk utstyr på bakgrunn av EU forordning for medisinsk utstyr: https://ec.europa.eu/docsroom/documents/38941

2.3 Personvernforordningen og personopplysnings-loven

Når det behandles helse- og personopplysninger i det medisinske utstyret vil personvernforordningen gjelde på samme måte som ved all annen behandling av helse- og personopplysninger.

2.4 Helselovgivningen

2.4.1 Pasientjournalloven

Pasientjournalloven § 22 stiller krav til den dataansvarlige og databehandleren som gjennom tekniske og organisatoriske tiltak skal sørge for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. personvernforordningen artikkel 32. Dette omfatter bl.a. å sørge for tilgangsstyring, logging og etterfølgende kontroll ved behandling av helse- og personopplysninger.

2.4.2 Helsepersonelloven

Loven inneholder bl.a. taushetspliktbestemmelser, og forbud mot "snoking", samt

[5] EU2017/745 av 5 april 2017 om medisinsk utstyr vedlegg 1, kapittel 2 nr. 17.

bestemmelser om kommunikasjon av helseopplysninger i forbindelse med helsehjelp. For en komplett oversikt se Helsedirektoratets rundskriv om helsepersonelloven.[6]

2.4.3 Pasient- og brukerrettighetsloven

Loven gir pasienter og brukere rett til retting, sletting og sperring av opplysninger, innsyn mv. i journal, samt vern mot spredning av egne helse- og personopplysninger. For en komplett oversikt se Helsedirektoratets rundskriv om pasient- og brukerrettighetsloven.[7]

2.4.4Taushetsplikt

Pasient/bruker skal kunne være sikker på at helse- og personopplysninger fra medisinsk utstyr ikke blir gitt videre til uvedkommende. Personell som behandler slike opplysninger er derfor underlagt taushetsplikt. Taushetsplikten følger av en rekke ulike bestemmelser, avhengig av hvilken rolle vedkommende personell har.

Helsepersonell er underlagt taushetsplikt etter helsepersonelloven når det gjelder pasientens legems- eller sykdomsforhold, samt andre personlige forhold personellet får vite om i egenskap av å være helsepersonell. Pasientjournalloven viderefører denne taushetsplikten til alle som får adgang til eller kunnskap om helseopplysninger fra et behandlingsrettet helseregister. Alle som behandler helse- og personopplysninger fra eller får tilgang til slike opplysninger fra medisinsk utstyr er derfor underlagt taushetsplikt.

Taushetsplikten er ikke til hinder for at helsepersonell kan få utlevert helse- og personopplysninger eller få tilgang til slike opplysninger når de har tjenstlig behov, jf. helsepersonellovens regler om tilgang til og utlevering av helseopplysninger.

[6] https://www.helsedirektoratet.no/tema/helsepersonelloven
[7] https://www.helsedirektoratet.no/tema/pasient-og-brukerrettighetsloven

3. Ansvar og styring

3.1 Inkludering av MU i styringssystem for informasjonssikkerhet (ledelsessystem)

Normen sier i kapittel 5.3.6 at medisinsk utstyr som behandler helse- og personopplysninger skal inkluderes i virksomhetens arbeid med informasjonssikkerhet, herunder i risikovurderinger, tilgangsstyring, endringskontroll og rutiner for bruk, på linje med andre informasjonssystemer.

For mer informasjon om styringssystem (ledelsessystem) for informasjonssikkerhet, se Normens kapittel 2, og veileder om internkontroll for informasjonssikkerhet og personvern

Noen dokumenter og områder i styringssystemet der MU bør inkluderes:

- Ansvar for forvaltning av MU synliggjøres i beskrivelse av sikkerhetsorganisasjonen. Hvis det er etablert egne sikkerhetsfunksjoner knyttet til MU (f.eks. medical it-network risk manager) skal dette fremgå av beskrivelsen.
- Virksomheten bør etablere faste samarbeidsfora mellom miljøene som er ansvarlig for sikkerhet, MU og IKT. Hvis virksomheten har etablert et sikkerhetsforum, bør representanter for forvaltning av MU inngå her. Klinisk side bør også være representert.
- Leverandører av medisinsk utstyr som f.eks. yter fjernsupport eller supporttjenester på MU som behandler helse- og personopplysninger bør inngå i oversikt over leverandører.
- MU og systemer som benyttes i tilknytning til MU som behandler helse- og personopplysninger, skal inngå i protokoll over behandlinger av helse- og personopplysninger.
- Nødvendige avtaler med leverandører skal være på plass, f.eks. databehandleravtaler.
- MU skal inkluderes i den gjennomførende delen av styringssystemet, f.eks.:
    - Opplæring og bevisstgjøring
    - Tilgangsstyring og hendelsesregistrering
    - Rutiner for bruk
- MU skal inkluderes i den kontrollerende delen av styringssystemet.
    - Avviksbehandling ved brudd på informasjonssikkerheten og personopplysningssikkerheten:
      Dersom bruddet har medført middels eller høy risiko for den registrerte, skal avviket rapporteres til Datatilsynet innen 72 timer. Dette inkluderer avvik som fører til utilsiktet, eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret, eller på annen måte behandlet. Virksomhetene må også være oppmerksom på at hendelser som

skyldes informasjonssikkerhetsbrudd kan være aktuelle å melde etter retningslinjer for meldeplikt etter forskriftene om medisinsk utstyr[8].

- Inkludere MU i virksomhetens sikkerhetsrevisjoner, f.eks. ved etterkontroll av gjennomførte sikkerhetstiltak.
- Inkludere MU i gjennomføring av risikovurderinger. Det er vesentlig å involvere klinisk ansvarlige i risikovurderingene.
- Inkludere MU i ledelsens gjennomgang, f.eks. ved å diskutere hvilke deler av den medisinske utstyrsparken der sikkerhetstiltak skal prioriteres etter gjennomførte risikovurderinger.

3.2 Dataansvar

Dataansvarlig er den som bestemmer formålet med behandling av helse- og personopplysninger og hvilke hjelpemidler som skal brukes. Ved bruk av MU vil dataansvarlig være virksomheten som bruker utstyret ved pasientbehandlingen. Det kan være helseforetak, fastlege, kommune eller privat tjenesteyter som har valgt å ta i bruk MU som ledd i pasientbehandlingen. Dersom dataansvarlig er en juridisk person (en virksomhet) er den juridiske personen behandlingsansvarlig, og ikke enkeltpersoner internt i virksomheten. Virksomhetens ledelse skal sørge for å etablere roller og funksjoner med tilstrekkelige ressurser og kompetanse til å gjennomføre nødvendige oppgaver for å ivareta ansvaret. Oppgavene kan utføres av egne ansatte eller av eksterne, men ansvaret kan aldri delegeres.

Noen av pliktene som påligger dataansvarlig:

- Dataansvarlig har plikt til å sørge for tilfredsstillende informasjonssikkerhet og personvern, dette omfatter også bruk av medisinsk utstyr. Dette innebærer bl.a. å sørge for å etablere og etterleve styringssystemet.
- Gjennomføre risikovurderinger og personvernkonsekvensvurderinger der det er nødvendig.
- Sikre den registrertes rettigheter.
- Etablere og dokumentere tekniske og organisatoriske tiltak.
- Inngå og følge opp avtaler.
- Håndtere avvik.

3.3 Behandlingsgrunnlag

Helse- og personopplysninger kan bare behandles når lovgivningen tillater det. All behandling av opplysninger skal ha et lovlig grunnlag i personvernforordningen. Dette kalles behandlingsgrunnlag. Behandlingsgrunnlaget skal dekke alle typer behandlinger av helse- og personopplysninger som utføres: innsamling, registrering, lagring, sletting, utlevering, mv.

8 https://legemiddelverket.no/Documents/Medisinsk%20utstyr/Melding%20om%20u%C3%B8nskede%20hendelser/Retningslinje%20for%20meldeplikt%20medisinsk%20utstyr.pdf

Skal opplysningene brukes til et annet formål enn det opprinnelige, må dette formålet ha et eget behandlingsgrunnlag.

Plikten til å føre journal gir virksomheten en rettslig plikt til å behandle helse- og personopplysninger ved ytelse av helsehjelp. Størstedelen av behandlinger av personopplysninger i helse- og omsorgssektoren er dermed lovpålagt. I tillegg til krav om dokumentasjon har lovverket også en rekke andre regler om behandling, f.eks. om utlevering av helse- og personopplysninger, intern kvalitetssikring mv.

Andre behandlinger av personopplysninger i virksomheten kan ha andre behandlingsgrunnlag f.eks. ved forskning på data som er samlet inn via et medisinsk utstyr. Behandlingsgrunnlaget skal fastsettes før behandlingen av helse- og personopplysninger starter, eller ved endringer i behandlingen.

Les mer om formål og behandlingsgrunnlag i Formål og behandlingsgrunnlag (faktaark 56).[9]

3.4 Protokoll

Dataansvarlig og databehandler skal føre protokoll over sine behandlingsaktiviteter. Dersom relevant, skal også den dataansvarliges representant også føre protokoll over behandlingsaktiviteter som utføres under deres ansvar.

Se mer om hva en protokoll skal inneholde og eksempler på en protokoll i Normens Protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13).[10]

3.5 Den registrertes rettigheter

En av helsesektorens overordnede målsettinger å yte god og likeverdig helsehjelp. Både personvernrettigheter og andre pasient- og brukerrettigheter er viktige forutsetninger for at denne målsettingen skal nås.

Les mer generelt om dette i Normens Veileder for rettigheter ved behandling av helse- og personopplysninger.[11]

Pasienten har rett til innsyn i journalen med bilag uansett i hvilken type behandlingsrettet helseregister opplysningene behandles. Det ville si at så lenge helse- og personopplysninger lagres i MU vil pasienten ha rett til innsyn i disse.

Helse- og personopplysninger skal slettes fra MU når relevante og nødvendige opplysninger er nedtegnet i pasientjournalen, jf. pasientjournalforskriften. Innsyn i helse- og personopplysninger fra MU vil derfor i praksis som regel måtte gis ved innsyn i pasientjournalen.

[9] Formål og behandlingsgrunnlag (faktaark 56)
[10] Protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13)
[11] Veileder for rettigheter ved behandling av helse og personopplysninger

Medisinsk utstyr genererer til en stor grad kun rådata og relevante og nødvendige opplysninger tolkes av ansvarlig helsepersonell og nedtegnes i pasientjournalen. I tilfeller hvor pasienten ønsker innsyn i opplysninger lagret i MU må det derfor gis forklaringer til pasienten om hva dataene betyr. I mange tilfeller vil relevant og nødvendig informasjon kun kunne gis ved innsyn i pasientjournal hvor disse ble journalført. Det er derfor viktig å informere pasienten om dette.

Pasienten har også rett til innsyn i hendelsesregister, eller logg, som viser hvem har hatt tilgang til eller fått utlevert opplysninger fra et behandlingsrettet helseregister. For MU kan det også være aktuelt å vise hendelsesregister over overføring av helse- og personopplysninger til pasientjournalen hvor slik logg finnes. Det vil i flere tilfeller ikke være mulig å vise slikt hendelsesregister i etterkant av bruk av MU ettersom ikke alt slikt utstyr kan føre slik logg. Når en pasient ber om innsyn i hendelsesregister for slikt utstyr må det forklares hvorfor slikt innsyn ikke er mulig.

Retten til retting og sletting vil også gjelde for medisinsk utstyr hvor det lagres helse- og personopplysninger.

3.6 Bruk av databehandler

Når eksterne leverandører behandler helse- og personopplysninger på vegne av dataansvarlig, f.eks. ved ekstern lagring eller sletting, er disse å anse som databehandlere. Databehandler kan ikke behandle helse- og personopplysninger på annen måte enn det dataansvarlig har bestemt.
For å regulere ansvar, rettigheter og plikter mellom dataansvarlig og databehandler, skal det inngås en databehandleravtale. Denne avtalen skal også regulere hvilke opplysninger databehandler skal behandle og for hvilket formål. I tilfeller hvor leverandøren skal bruke underleverandør(er) skal disse inngå en databehandleravtale som gjenspeiler avtalen mellom dataansvarlig og leverandøren, slik at de samme kravene som stilles til leverandøren også stilles til underleverandøren.

Databehandleravtalen skal inneholde krav om at ansatte hos leverandører skal undertegne en taushetserklæring på lik linje som ansatte i den dataansvarliges virksomhet. Dataansvarlig skal kunne se slike taushetserklæringer ved behov.
Bruk av databehandler (faktaark 10) gir ytterligere informasjon om bruk av databehandler, samt mal for databehandleravtale.

Ved anskaffelse av MU er det anbefalt å anskaffe utstyr hvor leverandøren ikke behandler helse- og personopplysninger eller i hvert fall begrense slik behandling til det som er absolutt nødvendig for tiltenkt bruk av utstyret.

I tilfeller hvor ekstern leverandør eller servicepersonell ikke skal behandle helse- og personopplysninger på vegne av dataansvarlig kreves det ikke en databehandleravtale. Innsyn i helse- og personopplysninger utløser i seg selv ikke behov for databehandleravtale. Det kreves ikke en databehandleravtale i tilfeller hvor ekstern leverandør eller servicepersonell bare skal utføre tjenesteoppdrag som omfatter installasjon, konfigurasjon, vedlikehold og andre tekniske tjenester som utføres av leverandøren på MU som eies, leies eller på annen måte disponeres av oppdragsgiveren. Dette er forutsatt at det ikke medfører databehandling ved at helse- og personopplysninger endres, kopieres eller hentes ut og

tilgangen ikke benyttes til medisinsk behandling eller diagnostikk. I slike tilfeller bør servicepersonell likevel undertegne taushetserklæring i tilfelle de kommer i kontakt med helse- og personopplysninger ved sitt arbeid, f.eks. utskrifter som ligger lagret i utstyret eller opplysninger på skjerm.

Det kan oppstå en gråsone der leverandøren har kontinuerlig fjerntilgang til systemer hvor personopplysninger behandles, og det må gjøres en konkret vurdering av hvorvidt det foreligger et databehandlerforhold.

3.7 Virksomhetens ansvar for informasjonssikkerhet når medisinsk utstyr tas i bruk

Driftsmiljøet for medisinsk utstyr er definert som ethvert IT/nettverksmiddel som samhandler med det medisinske utstyret som ikke leveres av produsenten av medisinsk utstyr.

Eventuelle minimumskrav til maskinvare, IT-nettverksegenskaper og IT-sikkerhetstiltak for driftsmiljøet bør defineres på grunnlag av risikovurdering for det medisinske utstyret, at det medisinske utstyret skal være så autonomt som mulig når det gjelder IT-sikkerhet, samt at produsentens forutsetninger for IT-sikkerhet i driftsmiljøet skal være dokumentert og referere til sikkerhetsstandarder for beste praksis.

Virksomheten må være i tråd med nasjonale og EU-regler (f.eks. GDPR).

Lagdelt sikkerhet bør normalt ikke kompensere for sårbarheter i medisinsk utstyr. Dersom medisinsk utstyr er avhengig av driftsmiljøet for viktige IT-sikkerhetskontroller, bør dette fremgå av den medfølgende tekniske dokumentasjonen.

Medisinsk utstyr bør brukes slik som produsenten har tiltenkt, i henhold til bruksanvisningen som følger med enhetene. Virksomheten bør følge produsentens publiserte krav og retningslinjer angående sikkerhet for igangkjøring, drift og demontering av medisinsk utstyr, f.eks. isolere et medisinsk utstyr fra internett hvis det ikke er nødvendig for bruken, bruke programvareoppdateringer i henhold til produsentens instruksjoner (når dette er virksomhetens ansvar) eller sørge for at programvare til beskyttelse mot skadelig kode er oppdatert, hvis det er aktuelt for utstyret.

Virksomheten må kontakte produsenten hvis passende sikkerhetsinformasjon ikke er tilgjengelig f.eks. i bruksanvisning, produsentens erklæring om medisinsk utstyrssikkerhet (MDS2) eller installasjonsveiledning.

Virksomheten er ansvarlig for anskaffelsen og bør sørge for at sikkerheten opprettholdes under drift og bruk av systemet (medisinsk utstyr), og spesielt at det ikke blir kompromittert av endringer i IKT-driftsmiljøet eller av brukerinteraksjon. Noen viktige momenter er:

- Forsikre deg om at det er et nødvendig sikkerhetsnivå for driftsmiljøet (nettverk, fysisk).
- Tilrettelegg nødvendig infrastruktur (nettverk, fysisk).
- Sørg for at brukerne er gitt nødvendig opplæring og er tilgjengelige i tilfelle sikkerhetsproblemer.
- Forsikre deg om at systemet brukes som beskrevet i produsentens retningslinjer (f.eks. ikke fysisk tilgang av uautoriserte brukere, passordpolicyer overholdes, tiltak for nettverkssikkerhet).

• Forsikre deg om at foreskrevet vedlikehold utføres etter behov, inkludert installasjon av sikkerhetsoppdateringer.

• Informer produsenten omgående ved mistanke om sikkerhetshendelser.

(Momentene er hentet fra dokumentet "MDCG 2019-16 Guidance on Cybersecurity for medical devices", utgitt desember 2019 av Medical Device Coordination Group, se https://ec.europa.eu/docsroom/documents/41863)

3.8 Leverandører og databehandlere

Produsenten av medisinsk utstyr har ansvar for at utstyr fungerer etter hensikten. Dette innebærer at forvaltning av MU som regel vil innebære tett samarbeid mellom virksomheten og produsentene/ leverandørene. Service på stedet er vanlig, men også ulike typer fjernovervåkning og fjernsupport benyttes. I de tilfeller leverandøren har som formål å behandle helse- og personopplysninger på vegne av virksomheten vil også leverandøren ha rollen som databehandler. Da må det inngås en databehandleravtale.

I dette kapitlet omtales fire områder av sikkerhetsmessig betydning ved samarbeid med leverandører: Anskaffelser, service og support fysisk hos virksomheten, fjernsupport og bruk av databehandler. Oppfølging av leverandører er et viktig område. Godt samarbeid mellom alle interessenter (f.eks. medisinsk-teknologisk avdeling, IKT og Innkjøpsfunksjonen) og gode rutiner fra anskaffelse til utfasing av utstyr er vesentlig.

3.8.1 Krav til informasjonssikkerhet og personvern til medisinsk utstyr ved anskaffelser

I forbindelse med anskaffelser vil en virksomhet ofte ha en god mulighet til å stille sikkerhetskrav overfor mulige leverandører av medisinsk utstyr. Krav til informasjonssikkerhet vil være en av flere typer krav. Selv om kravene til funksjon og bruk naturlig vil veie tyngst, så bør likevel relevante krav til informasjonssikkerhet inngå.

Som et utgangspunkt for krav til leverandører anbefales det å bruke vedlegget til Normen med oversikt over Normens krav med mapping mot ISO27001 (begge veier) og mapping av CCM: https://ehelse.no/normen/oversikt-over-normens-krav-og-mapping-mellom-iso-og-normen

Videre kan veilederen MDCG-2019-16 brukes for å finne relevante sikkerhetskrav som kan stilles ved anskaffelse av medisinsk utstyr. Veilederen beskriver hvordan produsenter av medisinsk utstyr kan oppfylle relevante krav til informasjonssikkerhet i Annex 1 i MDR og IVDR.[12] Mange av kravene som stilles i veilederen kan være egnet å ta inn i kravspesifikasjoner ved anskaffelser. Eksempler på krav som kan stilles til produsenten (med referanse til MDCG-2019-16) kan være:

- Sikkerhetskapabiliteter som må være på plass (kap. 3.3),
- systemer for rapportering av sikkerhetsrelaterte hendelser og distribusjon av sikkerhetsoppdateringer knyttet til utstyret (kap. 3.8), og
- dokumentasjon og brukerdokumentasjon knyttet til informasjonssikkerhet (kap. 4).

[12] Se kapittel 2 for nærmere omtale.

For nettverkstilknyttet utstyr er det i tillegg relevant å ta med krav som er mer direkte knyttet til muligheten for å sikre MU som skal anskaffes mot digitale angrep. Her kan anbefalinger fra amerikanske myndigheter (FDA) være et nyttig utgangspunkt for kravspesifikasjoner. FDA kommer med flere anbefalinger om sikkerhetstiltak som produsenter av medisinsk utstyr bør gjennomføre, anbefales det bl.a. tiltak knyttet til tilgangskontroll, integritet for kode og data, motstandsdyktighet mot digitale angrep, og dokumentasjon.[13] Av dokumentasjon som anbefales er bl.a. risikovurderinger og beskrivelse av hvordan softwareoppdateringer og beskyttelse mot skadelig kode skal ivaretas.

Anskaffelser skal alltid foregå i tett samarbeid med medisinsk-teknologiske avdelinger og klinikker. Forskrift om håndtering av medisinsk utstyr krever at utstyret skal være vurdert av brukere og teknisk personell for det tiltenkte området før anskaffelsen kan gjennomføres. En innkjøper skal derfor aldri anskaffe noe utstyr uten at dette er faglig klarert av bruker og medisinsk tekniske avdelinger.

3.8.2 Fysisk service og support

Det bør foreligge en skriftlig avtale mellom leverandøren og virksomheten som regulerer fysisk service og support. Dette gjelder både service som fortas hos virksomheten og service hos leverandøren.

Leverandørens ansatte som utfører arbeidet skal undertegne taushetserklæring. Det er ikke nødvendig at virksomheten administrerer taushetserklæringene for leverandørens ansatte. Dette kan gjøres av leverandøren selv, men virksomheten skal ha rett til innsyn.

Det kan være andre forhold som bør reguleres enten i serviceavtalen eller i instruks/erklæring. Dette kan være f.eks. endringshåndtering, varsling ved fremmøte, om leverandørens representant skal følges i spesielle områder, sikkerhet ved tilkobling av egen PC eller minnepinner, samt utkopiering av feillogger som kan inneholde helse- og personopplysninger.

I tilfeller der utstyr må sendes fysisk til leverandøren, og utstyret inneholder helse- og personopplysninger som ikke kan slettes, anbefales det å inngå en databehandleravtale med leverandøren. Forsendelsen må foregå på en sikker måte, f.eks. rekommandert sending.

[13] FDA, 2014: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices-0

4. Sikkerhetstiltak

Dette kapitlet omtaler en del sentrale bestemmelser, virkemidler og sikkerhetstiltak som er sentrale når en virksomhet skal sikre et tilstrekkelig nivå av informasjonssikkerhet og personvern ved bruk av medisinsk utstyr.

Det henvises til faktaark og veiledere som inneholder utdypende informasjon. Relevansen av tiltak og løsninger i disse støttedokumentene må vurderes ut fra en samlet og konkret risikovurdering av det medisinske utstyret som skal sikres. Dette er beskrevet nærmere i kapittel 5.

4.1 Fysisk sikring

Lagringsenhet for medisinsk utstyr som behandler helse- og personopplysninger skal plasseres fysisk sikring av områder og utstyr (faktaark 17)

Driftsmiljøet må gi medisinsk utstyr fysisk sikkerhet via sikkerhetstiltak som:

- Regulert og godkjent fysisk tilgang håndhevet via egnede tekniske tiltak (f.eks. adgangskort).
- Fysisk sikkerhetspolicy som definerer roller og tilgangsrettigheter, inkludert for fysisk tilgang til det medisinske utstyret.
- Bruk av adskilte, sikre områder med passende tilgangskontroller.

4.2 Opplæring og kompetanse

Alle virksomheter i helsesektoren skal iverksette tiltak for å lære opp medarbeiderne i informasjonssikkerhet og personvern, og i bruk av de ulike informasjonssystemene. Det er virksomhetens ledelse som har ansvaret for å tilrettelegge og sørge for at dette gjennomføres. For en generell omtale av opplæring i informasjonssikkerhet vises det til Veileder om internkontroll for informasjonssikkerhet og personvern.

Aktuelle målgrupper for opplæring i informasjonssikkerhet og personvern knyttet til medisinsk utstyr kan være brukere av MU, servicepersonell og IKT-personell.

Brukere av medisinsk utstyr vil trenge opplæring i rutiner for bruk av utstyret på en måte som ivaretar informasjonssikkerheten og personvernet til den registrerte. Dette vil være hensiktsmessig å gjennomføre som en integrert del av opplæring i korrekt og sikker bruk av utstyret. Virksomheten er pålagt å gjennomføre slik opplæring i henhold til forskrift om håndtering av medisinsk utstyr § 8, og skal blant annet gjennomføres ved nyanskaffelse, nyansettelse, bruk av vikar og vedlikeholdsopplæring.

Servicepersonell og personell som forvalter medisinsk utstyr vil trenge opplæring i informasjonssikkerhet og personvern på samme nivå som IKT-personell. Det bør være et mål at slike ansatte får god kjennskap til både sikkerhetskrav for spesifikt utstyr, generelle sikkerhetskrav, samt virksomhetens styringssystem for informasjonssikkerhet. Slik kan de fagmiljøene som forvalter MU i det daglige, også ta ansvar for informasjonssikkerheten rundt

utstyret. Hvis det er utpekt funksjoner med særlig ansvar for IKT og informasjonssikkerhet innen avdelingene med ansvar for forvaltning av MU, vil disse rollene kreve tyngre kompetanse innen informasjonssikkerhet, f.eks. innen gjennomføring av risikovurderinger.

IKT-personell og personell innen informasjonssikkerhet vil ofte samarbeide med ansvarlige for forvaltning av MU. I konkrete prosjekter krever dette forståelse for funksjonen til det medisinske utstyret som inngår. Endringer som påvirker MU og tilhørende systemløsninger kan medføre feil som påvirker utstyret/løsningens tiltenkte anvendelse og funksjonalitet. Det er derfor viktig at IKT-personell og sikkerhetspersonell har forståelse for særkravene i forskrifter til personell som skal reparere og vedlikeholde medisinsk utstyr.

4.3 Sikkerhetstiltak ved datalagring

Et sikkerhetstiltak som bør vurderes er om pseudonymiserte data kan benyttes i løsningen, f.eks. at data knyttes til stuenummer og tid, fremfor pasientidentifikasjon. Her må imidlertid behovet for sikker identifisering av pasienten vurderes og veie tungt. Hvis det er forsvarlig og praktisk mulig å ikke identifisere pasienten direkte i registreringen av kliniske data, vil dette spille inn i risikovurderingen av informasjonsbehandlingen (selv om også pseudonymiserte personopplysninger er personopplysninger).

Lagring av opplysninger som ikke lenger er nødvendige og relevante i MU vil være overskuddsinformasjon. Dette bør være et område som vurderes, og der det ved behov treffes tiltak. Jevnlig manuell sletting er eksempel på tiltak.

Behovet for sikkerhetskopiering av data som lagres på MU og tilhørende systemer må klarlegges gjennom risikovurderingen. Her er konfigurasjonsstyring av stor betydning, så endring av servernavn osv. ikke medfører at sikkerhetskopieringen utilsiktet faller ut. Tilbakelegging av data (restore) må testes jevnlig.

Et annet risikomoment er at helse- og personopplysninger kommer på avveie gjennom avhending eller utfasing av utstyr. Virksomheten må ha rutiner for sikker sletting. Se Håndtering av lagringsmedia (faktaark 34)

4.4 Tilgangsstyring

Formålet med tilgangsstyring er å sikre at helse- og personopplysninger kun er tilgjengelig etter tjenstlig behov. Dette innebærer at brukere autentiseres på en betryggende måte, og at tilganger tildeles, administreres, kontrolleres og fjernes.

For utfyllende informasjon om tilgangsstyring vises det til Normen kapittel 5.2 og Tilgangsstyring (faktaark 14).

Det må vurderes i hvilket omfang tilgangsstyring skal tas i bruk for MU for å sikre at kun personell med tjenstlig behov får tilgang til helse- og personopplysninger. Bruksscenariene i kapittel 5 er et utgangspunkt for vurdering av behovet for tilgang og forholdsmessig sikkerhet. I mange tilfeller vil fysisk sikring av utstyret innebære tilstrekkelig sikring, mens komplekse fagsystemer med store datamengder vil kreve tilgangsstyring på samme nivå som virksomhetens elektroniske pasientjournalsystem. For en del typer MU vil også rask tilgang til utstyret være avgjørende, slik at krav til innlogging ikke lar seg gjennomføre.

Tilgangsstyring avhenger av autentisering og autorisering. Autentiseringen innebærer at brukeren må identifisere seg overfor IKT-løsningen via en autentiseringsmekanisme som

brukernavn/passord, smartkort o.l. Autentiseringen skal sikre at rett person autoriseres og får tilgang til helse- og personopplysninger, og at hendelsesregistreringen viser hvem som faktisk har hatt tilgang. Autentiseringsmekanismen må være av tilstrekkelig kvalitet og styrke – og tildeling må skje på en betryggende måte. Sterke passord bør benyttes.

Ulike anvendelser vil stille ulike krav til styrken på autentiseringen. Intern pålogging til et fagsystem knyttet til MU vil kreve individuelle brukernavn og passord, mens ekstern pålogging vil kreve sterkere autentisering i tråd med Normens kapittel 5.2.1. For frittstående MU er det ofte ikke hensiktsmessig å benytte pålogging, men heller sikre informasjonen gjennom fysisk sikring. Som et minimum bør likevel bruk av hardkodede passord unngås.

Autorisering innebærer tildeling, administrering og kontroll av tilgang til informasjon i IKT-systemet. Ulike tilgangsnivåer basert på rollestyring (f.eks. «lege» og «administrator») er en vanlig mekanisme for tilgangsstyring. Tildeling av ulike roller til individuelle brukere er som regel aktuelt i større fagsystemer tilknyttet MU. For alle typer MU bør tilgang til administratorrettigheter begrenses.

Konsolidering av systemer tilknyttet MU, f.eks. sammenslåing av avdelingsvise databaser til et felles system for hele sykehuset, vil ofte medføre behov for mer fingranulert tilgangsstyring for å sikre at tilgang til helse- og personopplysninger skjer etter tjenstlig behov.

Krav til tilgangsstyring for MU er ikke et «særnorsk» krav. I sin «Content of Premarket Submissions for Management of Cybersecurity in Medical Devices» fra FDA (oktober 2014) anbefales følgende sikkerhetstiltak for å begrense tilgang kun til autoriserte brukere:

- Begrens tilgang til utstyr gjennom autentisering av brukere (f.eks. brukernavn og passord, smartkort og biometri).
- Bruk automatisk avslutning av inaktive sesjoner etter en viss tid.
- I tilfeller der det er hensiktsmessig, bruk rollebasert tilgangsstyring (f.eks. «helsepersonell» og «administrator»).
- Krav om sterkere autentisering for privilegert tilgangsnivå (administratorer og servicepersonell).
- Unngå hardkodede passord og beskytt tilgang til passord for privilegert tilgangsnivå.
- I tilfeller der det er hensiktsmessig, bruk fysisk sikring på utstyr og kommunikasjonsporter for å hindre at utstyret tukles med.
- Krev autentisering eller andre sikkerhetstiltak for å sikre at programvareoppdateringer på utstyret er autorisert.

Dette kan være krav som kan tas inn i kravspesifikasjoner ved anskaffelser av MU.

4.5 Hendelsesregistrering

Pasient/bruker har rett til å få innsyn i hvem som har hatt tilgang til helse- og personopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer. Dette vil fremgå av hendelsesregisteret. I tillegg skal virksomheten selv aktivt bruke hendelsesregisteret for å avdekke uautorisert tilgang (snoking). Hendelsesregistrering og oppfølging er nærmere omtalt i Innsyn i hendelsesregistre (faktaark 50).

Hendelsesregistrering er aktuelt der det samtidig benyttes tilgangsstyring. Uten individuell pålogging med unik identifikasjon av brukere er det ikke mulig si noe sikkert om hvem som har hatt tilgang til pasientens helseopplysninger.

4.6 Nettverkssikkerhet og tiltak mot skadelig kode

Når digitale angrep mot MU er et mulig trusselscenario må det gjennomføres tiltak som sikrer utstyret mot ondsinnet programvare. Dette kan skje på ulike måter, bl.a.:

- Anti-virus programvare.
- Holde utstyret jevnlig oppdatert med programvareoppdateringer.
- Bruk kun ekte programvare (fra sikre kilder).
- Ikke tildel sluttbrukere administrator-rettigheter.
- Blokker kjøring av ikke-autoriserte programmer («hvitelisting»).[14]
- Segmentere MU på dedikerte nettverk. Kommunikasjon inn og ut av dette nettverket begrenses og kontrolleres.
- Trafikkfiltrering.

Selv om MU som er sårbart for ondsinnet programvare er plassert på lukkede nett, kan skadelig kode spre seg via f.eks. minnepinner som blir brukt til å patche/oppdatere systemer. Antivirus-programvare og jevnlig programvareoppdatering kan derfor være et aktuelt tiltak også for utstyr som er adskilt fra øvrige nettverk. Kun programmer som er nødvendige for tiltenkt bruk bør installeres i driftsmiljøet. Virksomheten må ha rutiner for å sikre at sikkerhetsoppdateringer for driftsmiljøet (operativsystemer, applikasjoner, firmware mv.) og for medisinsk utstyr gjennomføres jevnlig og i tide.

For å planlegge og opprettholde sikkerhetstiltak mot digitale angrep, er det nødvendig å ha oversikt over konfigurasjon og dataflyt. Dette er en forutsetning både for gode nok risikovurderinger, og for effektiv konfigurasjonsstyring.

I tråd med anbefalinger fra FDA bør produsenten fremlegge dokumentasjon for hvordan dette skal ivaretas i hele utstyrets levetid. [15] Dette er særlig aktuelt å stille krav til i forbindelse med anskaffelser. Anbefalingene inneholder også noen momenter som er relevante for programvareoppdateringer:

- Krav til kodesignatur for programvareoppdateringer.
- Systematiske rutiner for hvordan oppdateringer skal skje.
- Mulighet for sikkerhetsmonitorering av MU.
- Informasjon til sluttbruker om hva vedkommende skal gjøre ved mistanke om sikkerhetsbrudd knyttet til utstyret.
- «Fail-safe» modus for utstyret, slik at kritisk funksjonalitet opprettholdes selv ved et digitalt angrep.

[14] Se f.eks. https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-01-fire-effektive-tiltak-mot-dataangrep.pdf

[15] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA, oktober 2014

- Mulighet for at en autorisert bruker kan rulle tilbake opprinnelig konfigurasjon ved behov.

I tilfeller hvor MU kommuniserer over eksterne nettverk virksomheten ikke har kontroll med selv, skal kommunikasjonen krypteres. Det vises til Kommunikasjon over åpne nett (faktaark 24). Et eksempel på dette kan være streaming av lyd og bilde fra operasjonsstue til annen lege utenfor helseforetaket eller i et annet land for second opinion eller veiledning.

4.7 Fjernsupport

Følgende krav bør legges til grunn:

- Etablering av løsning for fjernsupport og løsningsvalg skal være forankret i virksomhetens styringssystem, behov, og risikovurdering.
- Det skal foreligge skriftlig avtale med leverandør.
- Følgende dokumentasjon skal foreligge:
    - Signert taushetserklæring med henblikk på tilgang til helse- og personopplysninger. Leverandøren oppbevarer disse for eget personell.
    - Lest og akseptert sikkerhetsinstruks.
    - Nødvendige rutiner (f.eks. opplæring, autentisering, autorisasjon, avviksbehandling, hendelsesregistrering, sletting, oppgaver ved oppkobling og kontroll).
- Valg og etablering av teknisk løsning
    - Den ytre termineringen bør skje gjennom en brannmur og i en egen DMZ-sone for fjernaksess.
    - Kun forhåndsgodkjent og eksplisitt definert trafikk tillates.
    - Det anbefales autentisering med høyt sikkerhetsnivå. Risikovurderingen skal vise at valgt autentiseringsløsning er sikker.
    - Om det foreligger et faglig behov for at leverandøren flytter helse- og personopplysninger til leverandørens sikre nettverksområder skal det utføres i henhold til en databehandleravtale.
    - All kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer, skal sikres ved kryptering.[16]
    - Det skal være løsninger for å hindre ondsinnet programvare hos leverandøren og virksomheten.
    - Det skal sikres med tekniske tiltak at leverandørens arbeidsstasjon ikke er tilkoblet andre nettverk når det gjennomføres tilkobling til virksomhetens nettverk.
- Det skal etableres hendelsesregistrering.

For utdypende informasjon om fjernsupport vises det til Normens Veileder for fjernaksess mellom virksomhet og leverandør.

[16] NSM Cryptographic recommendations https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/nsm-cryptographic-recommendations/

4.8 Skytjenester

I de tilfellene det lagres helse- og personopplysninger i skyen (eksterne serverparker som ofte er tilknyttet internett, se f.eks. bruksscenario 14), innebærer dette at leverandøren av skytjenesten har rollen som databehandler overfor dataansvarlig, og det kreves en databehandleravtale. For mer informasjon vises det til Normens veileder om skytjenester.

4.9 Tilgang til helseopplysninger utover virksomhetsgrenser

I henhold til pasientjournalloven kan det gis tilgang til helseopplysninger utover virksomhetsgrenser på to måter:

- To eller flere virksomheter kan samarbeide om felles journal som skal erstatte virksomhetenes interne journal. Dette vil være aktuelt hvis to eller flere virksomheter samarbeider om et felles fagsystem som benyttes i tilknytning til MU. Det vises til Normens kapittel 5.8.5 og Veileder med avtaleeksempler ved samarbeid om felles journal.
- Det kan etableres tilgang til helseopplysninger mellom virksomheter. Med tilgang menes at helsepersonell i en virksomhet gis adgang til direkte elektronisk å hente frem helseopplysninger om pasienter/brukere registrert ved en annen virksomhet. Dette er aktuelt hvis en bruker fra virksomhet A skal gis tilgang til å logge seg inn i fagsystem i virksomhet B – f.eks. for å bistå i tolkning av resultater. Det vises til Normens kapittel 5.2.1.2, og veilederen om tilgang til helseopplysninger mellom virksomheter.

I tillegg kan helseopplysninger utleveres fra en virksomhet til en annen, f.eks. gjennom meldingsutveksling.

4.9.1 Utlevering av helseopplysninger til utlandet

Helse- og personopplysninger kan overføres til land innen EU/EØS-området.

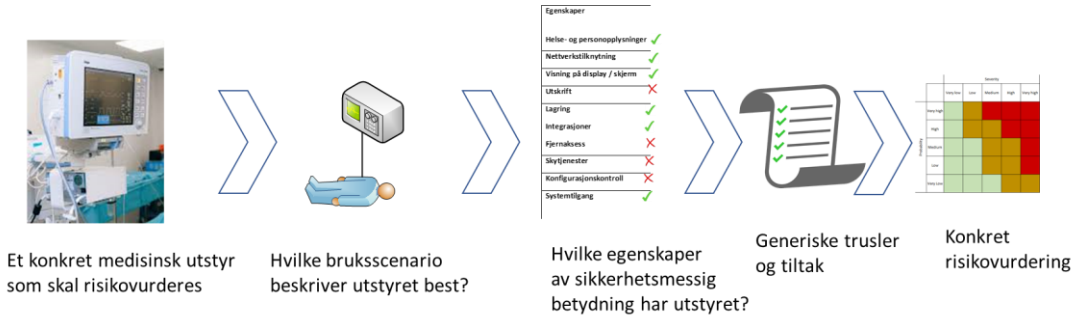
Dersom det skal benyttes leverandører eller tjenester etablert utenfor EU/EØS, kan det gjelde spesielle krav. Disse kravene skal sikre at opplysningene er underlagt samme beskyttelsesnivå som i EU/EØS-området. Når virksomheten overfører personopplysninger til stater utenfor EU/EØS-området, såkalte «tredjeland», skal den bruke et av overføringsgrunnlagene i personvernforordningen artikkel 46. Se Datatilsynets veiledning.

5. Risikobilde ved behandling av personopplysninger i medisinsk utstyr

5.1 Bruksscenarioer og egenskaper av sikkerhetsmessig betydning

For å kunne beskrive trusler og aktuelle sikkerhetstiltak er det hensiktsmessig å skille mellom ulike bruksscenarioer for medisinsk utstyr. I tillegg er det identifisert en del egenskaper av sikkerhetsmessig betydning for medisinsk utstyr.

Når trusler og tiltak skal vurderes for å sikre medisinsk utstyr, må en finne fram til hvilke bruksscenario og hvilke egenskaper som best beskriver løsningen. Ut fra bruk dette vil de generiske truslene og tiltakene som er beskrevet være et utgangspunkt for en risikovurdering av utstyret.

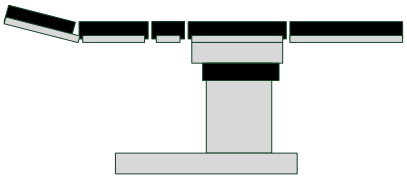


I kapittel 4 fremgår det hvilke sikkerhetstiltak som er relevante og kan la seg gjennomføre for de ulike bruksscenarioene og egenskapene.

Under er det beskrevet fem bruksscenarier, og deretter en nærmere beskrivelse av egenskaper av sikkerhetsmessig betydning.

5.1.1 Nærmere beskrivelse av bruksscenarier

Bruksscenario 1: Medisinsk utstyr uten behandling av informasjon



Eksempel:

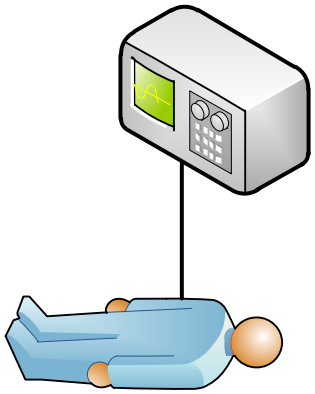
- Operasjonsbord

Parameter	«Ja» eller «Kan» indikerer sikkerhetsmessig betydning
Helse- og personopplysninger	Nei
Visning på display/skjerm	Nei
Utskrift	Nei
Lagring	Nei
Nettverkstilknytning	Nei
Integrasjoner	Nei
Fjernaksess	Nei
Skytjenester	Nei
Konfigurasjonskontroll	N/A

Trusselbilde: Ingen trusler innenfor det som omtales i denne veilederen.

Tiltak: Ingen tiltak innenfor det som omtales i denne veilederen.

Bruksscenario 2: Medisinsk utstyr ikke tilknyttet nettverk.



Eksempler:

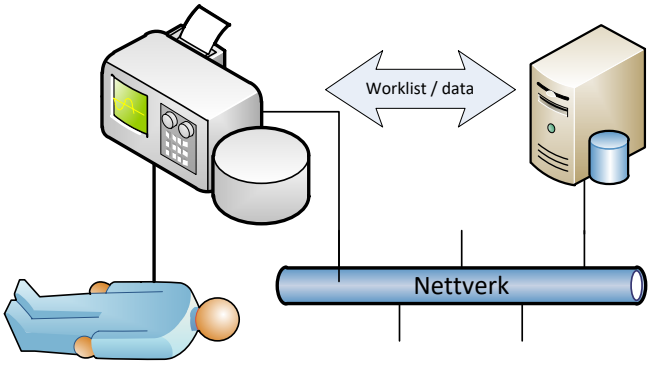
- Elektronisk blodtrykksapparat som måler blodtrykket og presenterer kun verdier i et display.
- CTG-apparat som måler hjertefrekvensen til et foster over tid og skriver det ut på papir, men data blir ikke lagret elektronisk.
- EKG-apparat som tolker EKG-data og produserer en rapport som kan skrives ut, og lagres elektronisk i et internt arkiv.
- Pulsmålere

Egenskaper	«Ja» eller «Kan» indikerer sikkerhetsmessig betydning
Helse- og personopplysninger	Ja
Visning på display/skjerm	Kan
Utskrift	Kan
Lagring	Kan
Nettverkstilknytning	Nei
Integrasjoner	Nei[17]
Fjernaksess	Nei
Skytjenester	Nei
Konfigurasjonskontroll	Leverandør kan ha fysisk tilgang og gjennom dette ha konfigurasjonskontroll

[17] Ikke via nett, men enkelte typer utstyr kan ha integrasjoner med f.eks EPJ via seriellport

Trusselbilde og tiltak: Er knyttet til aktuelle egenskaper (tabellen over) for bruksscenarioet. Se kapittel 5.1.2.

Bruksscenario 3: Medisinsk utstyr tilknyttet nettverk.



Dette omfatter:

- Overføring av data i lokale nettverk.

  MU overfører data i virksomhetens interne nettverk. Dette kan være et dedikert nettverk for MU, eller generelt IKT-nettverk.
- Overføring av data i eksterne nettverk.

  Det overføres data i nettverk som er utenfor virksomhetens kontroll, f.eks. internett eller helsenett.
- Teknisk overvåkning.

  Driftsstatus og andre tekniske parametere overføres fra utstyret i forbindelse med teknisk administrasjon og drift av utstyret. Dette kan omfatte f.eks. feilmeldinger, batteristatus og serviceintervaller opp mot faktisk bruk.
- Trådløs kommunikasjon.
- Dataoverføring internt eller eksternt skjer trådløst, f.eks. over mobile nett eller WLAN.

Eksempler:

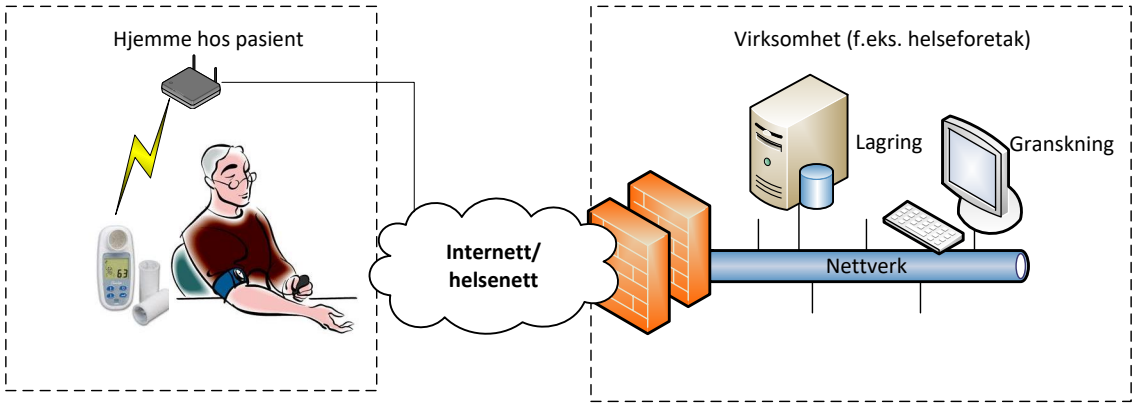
- Overvåkingssentralskop som viser pasientnavn og data på en eller flere skjermer.
- EKG-apparat som tolker EKG-data og produserer rapport som kan skrives ut. Den blir temporært lagret elektronisk i det interne arkivet fram til rapporten er lagret i det eksterne arkivet. Da blir alt slettet i det interne arkivet.
- CT som lagrer data som det blir generert bilder av. Data og bilder blir permanent lagret lokalt, mens bilder også blir lagret eksternt. (Årsaken til at data blir lagret internt er at det er kanskje bare det lokale utstyret som kan generere nye bilder fra eksisterende lokale data).

- MU som er plassert i ambulanser og sender data over mobilnettet til en server.

Egenskaper	«Ja» eller «Kan» indikerer sikkerhetsmessig betydning
Helse- og personopplysninger	Ja
Visning på display/skjerm	Kan
Utskrift	Kan
Lagring	Kan
Nettverkstilknytning	Ja
Integrasjoner	Kan
Fjernaksess	Kan
Skytjenester	Kan
Konfigurasjonskontroll	Kan være leverandør

Trusselbilde og tiltak: Er knyttet til aktuelle egenskaper (tabellen over) for bruksscenarioet. Se kapittel 5.1.2.

Bruksscenario 4: Behandlingshjelpemidler.



Eksempler:

- 24-timers blodtrykksapparat der det er en løs, standard minnebrikke som lagrer data. Når pasienten kommer inn på sykehuset igjen blir minnebrikken avlest. Alternativt 24-timers EKG der data lagres internt, og der avlesning skjer ved at det bærbare EKG-apparatet kobles til avlesningsstasjon. Data blir lagret internt i avlesningsstasjonen, og rapport kan lagres eksternt.
- MU som blir plassert hjemme hos pasient, og som sender data trådløst til et aksesspunkt i hjemmet. Data sendes videre til virksomheten for lagring/granskning.

- Alarmeringsteknologi, digitalt tilsynsløsninger som plasseres i pasientens hjem/ på pasient og sender data over mobilnettet til responssenterløsninger.
- GPS-klokker, apper på mobil/nettbrett og annen sporingsteknologi/ trygghetsteknologi som plasseres på pasienten som sender data over mobilnett til responssenterløsninger.
- Insulinpumpe utdelt til pasienten som tar det med seg hjem. Neste gang pasienten er på kontroll på sykehuset leser sykehuset ut trenddata av apparatet. Pasienten kan sende data fra det medisinske utstyret vedkommende har fått utlevert til fabrikant av MU som lagrer data hos seg, eventuelt i en skytjeneste.
- MU der data lastes opp til skytjeneste fra pasienten, og der tjenesten omfatter preprosessering[18] før resultatet oversendes virksomheten.

Egenskaper	«Ja» eller «Kan» indikerer sikkerhetsmessig betydning
Helse- og personopplysninger	Ja
Visning på display/skjerm	Kan
Utskrift	Kan
Lagring	Kan
Nettverkstilknytning	Ja
Integrasjoner	Kan
Fjernaksess	Kan
Skytjenester	Kan
Konfigurasjonskontroll	Kan være leverandør

Trusselbilde:

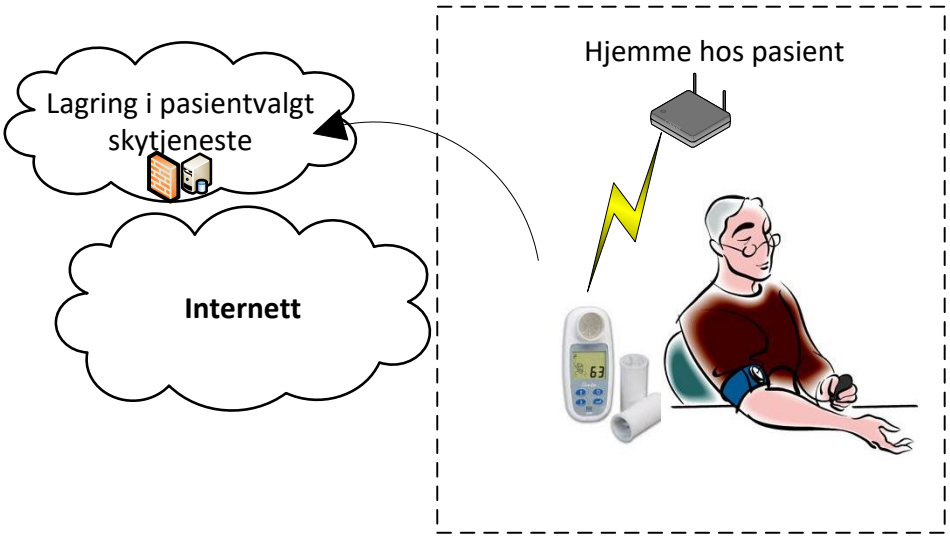
- Pasient mister minnekortet/lagringsmedium.
- Digitale angrep fører til at utstyret blir utilgjengelig og/eller tjener som brohode for slike angrep videre inn i infrastrukturen.

Tiltak:

Nettverkssikkerhet, sikkerhetsoppdateringer og tiltak mot skadelig kode (4.10).

[18] Omfatter ikke helsefaglige vurderinger som medfører journalføringsplikt

Bruksscenario 5: Pasienten tar selv i bruk tjenester fra produsenten av utstyret.



Eksempler:

Egenskaper	«Ja» eller «Kan» indikerer sikkerhetsmessig betydning
Helse- og personopplysninger	Ja
Visning på display/skjerm	Kan
Utskrift	Kan
Lagring	Kan
Nettverkstilknytning	Ja
Integrasjoner	Kan
Fjernaksess	Kan
Skytjenester	Kan
Konfigurasjonskontroll	Kan være leverandør

Trusselbilde:

- Utenfor dataansvarliges kontroll. Leverandør av utstyr som tilbyr tilleggsfunksjonalitet er dataansvarlig og skal baseres på samtykke fra pasient.

Tiltak:

- Tilstrekkelig dekkende databehandleravtale.
- Virksomheten som leverer ut teknologien ved ytelse av helse- og omsorgstjenester bør gi tilstrekkelig informasjon til pasient/bruker om ansvaret knyttet til ytelsen og dataansvaret.

Tilstrekkelige sletterutiner etter pasient/bruker leverer tilbake medisinske utstyret til sykehuset/kommunen.

5.1.2 Nærmere beskrivelse av egenskaper av sikkerhetsmessig betydning

1. Visning på skjerm/display	
Helseopplysninger vises på skjerm e.l. lokalt på utstyret	
Trusler:	Mulige tiltak:
• Innsyn fra uvedkommende	• Tilstrekkelig sikring mot innsyn fra uvedkommende • Fysisk sikring

2. Utskrift	
Utstyret har mulighet for utskrift av helseopplysninger	
Trusler:	Mulige tiltak:
• Innsyn fra uvedkommende • Sensitive utskrifter på avveie	• Tilstrekkelig sikring mot innsyn fra uvedkommende • Gode makuleringsrutiner • Fysisk sikring

3. Lagring	
Lagring av helse- og personopplysninger. Dette kan skje ved: • Intern lagring Helse- og personopplysninger lagres i utstyret. Lagringsplassen er som regel begrenset, slik at lagringen i de fleste tilfeller er temporær. • Ekstern lagring Helse- og personopplysninger lagres på ekstern lagringsmedium tilknyttet utstyret. Dette kan være f.eks. DVD eller en ekstern harddisk. • Serverbasert lagring Helse- og personopplysninger overføres fra utstyret til en nettverkstilknyttet server. Dette kan i enkleste form være lagring på et filområde, eller lagring i databaser tilknyttet et fagsystem. • Lagring hos databehandler/i skyløsning Se nærmere omtale av dette under.	
Trusler:	Mulige tiltak:
• Det bygges opp et behandlingsrettet helseregister uten at kravene i personopplysningslovverket eller helselovgivningens krav til	• Sikkerhetstiltak ved datalagring. • Tiltak som sikrer behandlingsgrunnlag. Behandlingen

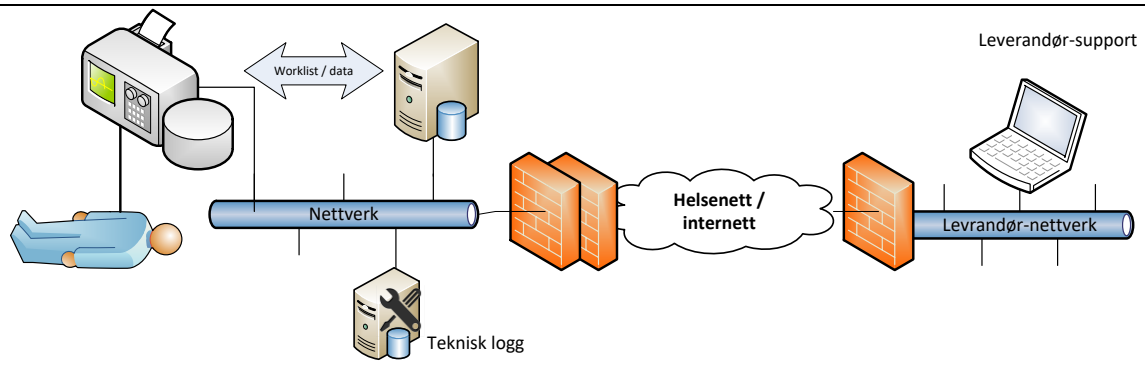
behandlingsrettede helseregistre følges. • Utstyr på avveie kan medføre tilgang til helse- og personopplysninger for uvedkommende. • Manglende tilgjengelighet til helseopplysninger ved lokale systemfeil. • Manglende tilgjengelighet til helseopplysninger ved nedetid i sentral infrastruktur. • Manglende tilgangsstyring. • Manglende logging. • Manglende backup. • Ved sentral datalagring, inkluderes ikke denne i backup. • Manglende sletting av opplysninger som anses som "overskuddsinformasjon". • Manglende rutiner for sletting når formål er oppnådd.	er ført i protokoll og at den registrertes rettigheter er ivaretatt. • Backup. • Tilgangsstyring på lokalt utstyr og sentrale systemer • Logging

4. Nettverkstilknytning	
• Overføring av data i lokale nettverk MU overfører data i virksomhetens interne nettverk. Dette kan være et dedikert nettverk for MU, eller generelt IKT-nettverk. • Overføring av data i eksterne nettverk Det overføres data i nettverk som er utenfor virksomhetens kontroll, f.eks. internett eller helsenett. • Teknisk overvåkning Driftsstatus og andre tekniske parametere overføres fra utstyret i forbindelse med teknisk administrasjon og drift av utstyret. Dette kan omfatte f.eks. feilmeldinger, batteristatus og serviceintervaller opp mot faktisk bruk. • Trådløs kommunikasjon Dataoverføring internt eller eksternt skjer trådløst, f.eks. over mobile nett eller WLAN.	
Trusler:	Mulige tiltak:
• Digitale angrep fører til at utstyret blir utilgjengelig og/eller tjener som brohode for slike angrep videre inn i infrastrukturen	• Nettverkssikkerhet, sørge for sikkerhetsoppdateringer, unngå unødvendig administratortilgang, gjennomføre tiltak mot skadelig kode. • Endre administratorpassord

• Manglende tilgjengelighet ved nedetid i nettverk/sentral infrastruktur • Manglende kryptering/sikring av trådløs kommunikasjon kan medføre uautorisert tilgang til opplysninger eller brudd på integritet • Manglende sikkerhetsoppdateringer gjør utstyret sårbart for angrep og skadelig kode	• Kryptering av trafikk • Sikring av trådløs kommunikasjon

5. Integrasjoner	
Medisinsk utstyr er integrert med andre systemer, f.eks. PACS/VNA, kurve eller EPJ. Data mottas fra integrerte systemer (f.eks. worklist) og/eller data sendes til integrerte systemer (for eksempel bilder, rapporter osv.)	
Trusler:	Mulige tiltak:
Misbruk av integrasjonsgrensesnitt for • uautorisert tilgang til helse- og personopplysninger • uautorisert ending av helse- og personopplysninger • uautorisert endring av styringsparametere på medisinsk utstyr • gjennom uautorisert tilgang forårsake manglende tilgjengelighet til medisinsk utstyr? (f.eks. indirekte ved av utstyret må tas ut av bruk for feilsøking, eller direkte ved at utstyret settes ut av funksjon ved sabotasje eller utilsiktet)	• Penetrasjontest av tilgang til medisinsk utstyr • Herding av integrasjonsgrensesnitt (• Sikring av API?

6. Fjerntilgang
Leverandør trenger VPN-tilgang til utstyret for å drive driftsovervåking, aktiv feilretting eller online brukerstøtte



Trusler:	Mulige tiltak:
• Uautorisert eksponering av helse- og personopplysninger hos leverandøren • Utilsiktet lagring av helse- og personopplysninger i tekniske logger • Leverandøren utfører operasjoner på systemer som medfører ikke- planlagt nedetid	• Kontroll på hvilke data som overføres til tekniske logger, sikring av logger • Sikring av leverandørtilgang (egen veileder) og Normens krav

7. Skytjenester	
En skytjeneste er en betegnelse for alt fra dataprosessering og datalagring til programvare på servere som står i eksterne serverparker, som vanligvis bruker Internett som bærer av datatrafikken. Tjenestene i skyen kjennetegnes ved at de er laget for dynamisk skalering ved kapasitetsbehov, og ved at det som regel betales for faktisk bruk. Leverandører tilbyr for eksempel serverkapasitet i skyen på timebasis.	
Trusler:	Mulige tiltak:
• Uautorisert tilgang til helse- og personopplysninger fra leverandøren • Utlevering av personopplysninger utenfor EU/EØS-området • Manglende databehandleravtale • Data slettes ikke ved opphør av avtale • "Sammenblanding" av ulike kunders data • Manglende tilgjengelighet ved feil • Manglende databehandleravtale • Leverandør benytter data til andre formål enn avtalt • Manglende sletting av overskuddsinformasjon	• Kryptering av data • Kontroll på hvilke data som overføres til tekniske logger, sikring av logger • Avtaler og sikkerhetstiltak ved bruk av databehandler (referanse) • Sikring av skytjenester (referanse) og egen veileder

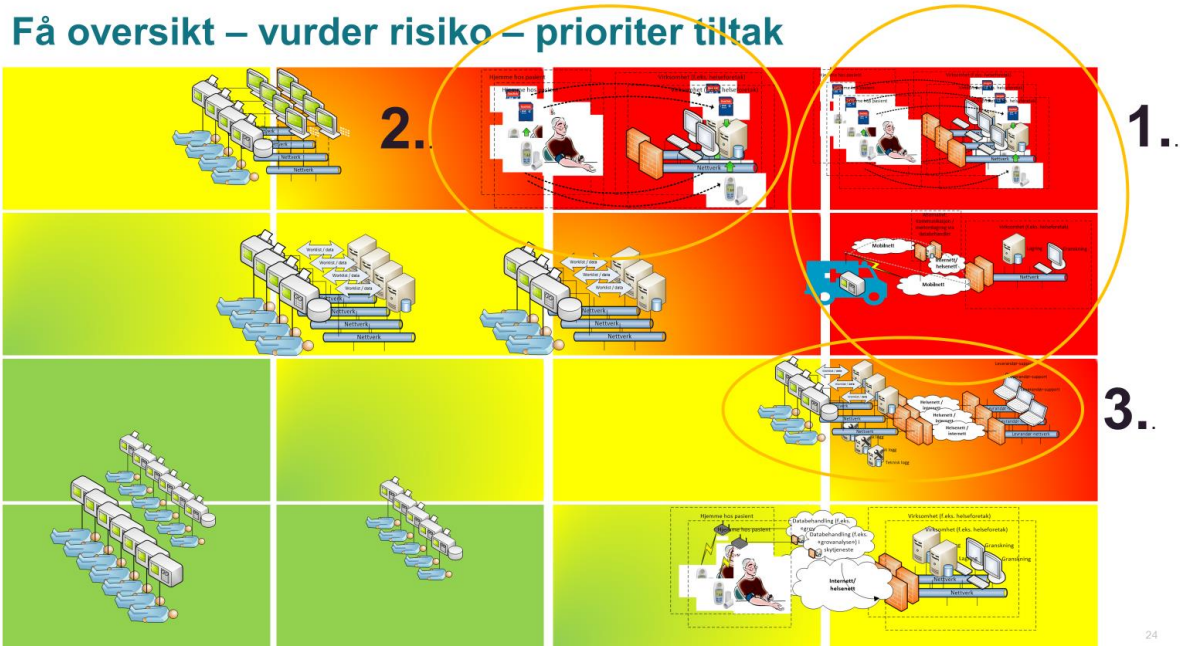
8. Konfigurasjonskontroll	
Beskriver hvor ansvaret for konfigurasjonskontroll er plassert – hos virksomheten, hos en eller flere leverandører, eller en kombinasjon. Konfigurasjonen skal sikre at utstyret og programvaren kun utfører de funksjoner som er formålsbestemt. Leverandøren kan ha tilgang til utstyr og systemer fysisk og/eller via fjernaksess.	
Trusler:	Mulige tiltak:
• Utstyret og programvaren utfører ikke kun de funksjoner som er formålsbestemt	• Regulere konfigurasjonskontroll gjennom avtale • Normens krav til konfigurasjonskontroll (kap. 5.4.1)

5.2 Risikobasert tilnærming

5.2.1 Risikostyring

Kravet i lovverket til informasjonssikkerhet er forholdsmessig sikring. Dette innebærer at sikkerhetstiltakene skal være tilpasset det fastsatte nivået for akseptabel risiko i virksomheten. Det første steget en virksomhet må ta for å kunne håndtere risiko på en systematisk og planlagt måte er å ha oversikt over hvilke informasjonsverdier eller informasjonsbehandlinger som skal sikres.

Alle virksomheter som forvalter medisinsk utstyr er pliktig til å ha oversikt over utstyret som virksomheten har ansvaret for. Denne oversikten er et godt utgangspunkt for en overordnet risikovurdering av informasjonssikkerhet i tilknytning til utstyret. Ved å ta utgangspunkt i brukstilfellene ovenfor, og sammenligne eget utstyr med disse, kan virksomheten gjøre en grovsortering av hvilke deler av den medisinske utstyrsparken som er mest utsatt for risiko, og der sikkerhetstiltak må vurderes først. I henhold til Normens kapittel 4.6 kan det i en overgangsperiode benyttes administrative tiltak, f.eks. i form av rutiner dersom tekniske tiltak for å oppnå akseptabel risiko ikke innføres umiddelbart.



En overordnet risikovurdering av utstyrs- og systemparken knyttet til medisinsk utstyr er et godt utgangspunkt for å prioritere videre risikovurdering og oppfølging.

En kan f.eks. si at utstyr som behandler pasientidentifiserbare data, og som er nettverkstilknyttet, og der leverandør har tilgang via VPN er mest eksponert for risiko, mens utstyr som ikke er nettverkstilknyttet er minst eksponert for risiko. Neste steg blir da å gjennomføre mer dyptgående risikovurderinger for det medisinske utstyret som er mest utsatt. I forbindelse med slike vurderinger kan metodikk fra standarder som IEC 80001 være til nytte.

Det er vesentlig å involvere klinisk ansvarlige i risikovurderingene, slik at man har oversikt over hva som er tiltenkt bruk av utstyret.

5.2.2 Kort om IEC 80001 Application of risk management for IT-networks incorporating medical devices

Denne standarden beskriver roller, ansvar og aktiviteter ved risikostyring når medisinsk utstyr tilknyttes virksomhetens IT-nettverk.[19] IT-nettverk defineres som et system eller systemer som består av kommunikasjonsnoder og transmisjonsforbindelser som gir fysisk tilkoblet eller trådløs kommunikasjon mellom to eller flere spesifiserte kommunikasjonsnoder. Et medisinsk IT-nettverk er et IT-nettverk som består av minst ett medisinsk utstyr.

[19] Hvis det leveres egne sertifiserte MU nettverksløsninger som en del av utstyret som benyttes (for eksempel hjerteovervåkingsnettverk) gjelder ikke standarden for disse. Her vil produsenten ha ansvar for risikovurdering. På dette området er standarder som ISO14971 aktuelle.

Standarden beskriver at «safety», «effectiveness» og «data and system security» skal adresseres i risikostyringen.[20] Disse tre begrepene er kalt «key properties» i standardene, og er i vår oversettelse definert på følgende måter: [21]

- «Safety», tilsvarende «trygghet», eller «sikkerhet» som det benyttes i konteksten HMS, eller pasientsikkerhet; Frihet fra uakseptabel risiko for tap av liv og helse, eller skade på eiendom eller miljø.
- «Effectiveness», evne til å skape ønsket resultat for pasient og virksomheten.
- «Data and system security», tilsvarende informasjonssikkerhet, informasjonsverdier er tilstrekkelig beskyttet mot tap av konfidensialitet, integritet og tilgjengelighet.

Standarden beskriver ansvar for virksomheten og virksomhetens ledelse. Videre vektlegges rollen «medical it-network risk manager». Denne rollen skal bl.a. kommunisere med alle interessenter i risikostyringsarbeidet. Dette inkluderer produsenter av medisinsk utstyr, IT-leverandører, medisinsk-teknologisk avdeling, interne tjenesteytere innen IKT og teknisk drift og kliniske brukere. Ansvar og oppgaver for produsenter av medisinsk utstyr og IT-leverandører er spesielt omtalt.

IEC 80001 tar videre for seg risikostyring i et livsløpsperspektiv for medisinske IT-nettverk.

Dette er knyttet opp mot endringsstyring slik det et beskrevet i andre standarder eller i ITIL.[22] Ved hver forespørsel om endring (f.eks. tilkobling av nytt medisinsk utstyr i IT-nettverket) skal det foreligge en endringsforespørsel. Et prosjekt risikovurderer endringen og oppdaterer risikodokumentasjonen («Risk management file»). Når restrisikoen er akseptabel kan endringen implementeres i tråd med rutinen for konfigurasjonsstyring. Etter at endringen er utført sikres akseptabel risiko gjennom monitorering og hendelsesstyring.

Dokumentasjon av ansvar for utførelse av oppgaver i hele prosessen vektlegges gjennom inngåelse av «responsibility agreements».

[20] For å risikovurdere informasjonssikkerhet og personvern ved *medisinsk utstyr* på en måte der det også tas hensyn til bl.a. *pasientsikkerhet*, kan en tenke seg at «safety» og «effectiveness» bringes inn som tilleggs- dimensjoner i risikovurderingen.

[21] Det foreligger ingen offisiell norsk oversettelse av standarden

[22] https://www.axelos.com/best-practice-solutions/itil

Endringshistorikk

Dato	Versjon	Endring
10.12.2015	1.0	Første utgave av veilederen
08.06.2017	1.1	Lagt til lenke til OUS IKT-/sikkerhetskrav i kap. 4.5.1 Lagt til tekst om veilederens forhold til EUs nye personvernforordning i kap. 1.3
11.06.2021	2.0	Revidert lovbestemmelser, brukerscenarier, tiltakene, samt endret strukturen. Definisjoner er fjernet, det vises til definisjonslisten i Normen.

Vedlegg

Grunnleggende prinsipper

Medical Device Coordination Group (MDCG) har i desember 2019 utgitt veilederen "MDCG 2019-16 Guidance on Cybersecurity for medical devices" som bl.a. beskriver grunnleggende prinsipper for digital sikkerhet for medisinsk utstyr. Nedenfor følger et utdrag av momenter som bør inngå i virksomhetenes arbeid for å oppnå godt sikkerhetsarbeid på dette området.

Medisinsk utstyr bør brukes slik som produsenten har tiltenkt, i henhold til bruksanvisningen som følger med enhetene. Virksomheten bør følge produsentens publiserte krav og retningslinjer angående sikkerhet for igangkjøring, drift og demontering av medisinsk utstyr, f.eks. isolere et medisinsk utstyr fra internett hvis det ikke er nødvendig for dets drift; bruke programvareoppdateringer i henhold til produsentens instruksjoner (når dette er virksomhetens ansvar), eller sørge for at programvare til beskyttelse mot skadelig kode er oppdatert, hvis det er aktuelt for utstyret.

Driftsmiljøet for medisinsk utstyr er definert som ethvert IT/nettverksmiddel som samhandler med det medisinske utstyret som ikke leveres av produsenten av medisinsk utstyr.

Eventuelle minimumskrav til maskinvare, IT-nettverksegenskaper og IT-sikkerhetstiltak for driftsmiljøet bør defineres på grunnlag av følgende prinsipper:

- Ethvert foreslått IT-sikkerhetskrav for driftsmiljøet bør være basert på risikovurderingen for det medisinske utstyret.
- Det medisinske utstyret skal være så autonomt som mulig når det gjelder IT-sikkerhet, og den eneste avhengigheten av at det eksisterer IT-sikkerhetskrav til driftsmiljøet, bør holdes på et minimum og gjenspeile produsentens antagelser om grunnleggende miljøsikkerhet for sikker drift av det medisinske utstyret.
- Produsentens forutsetninger om IT-sikkerheten i driftsmiljøet skal være tydelig dokumentert i bruksanvisningen og kan referere til sikkerhetsstandarder for beste praksis.
- I samsvar med prinsippet om lagdelt sikkerhet, bør IT-sikkerhetstiltak for driftsmiljøet generelt ikke tjene formålet med å kompensere sikkerhetskontroll for sårbarheter i medisinsk utstyr, med mindre det er tilstrekkelig begrunnelse. I tilfeller der medisinsk utstyr er avhengig av driftsmiljøet for å gi viktige IT-sikkerhetskontroller, bør dette fremgå av den medfølgende tekniske dokumentasjonen.

Produsenten av medisinsk utstyr bør bestemme IT-sikkerhetskravene for driftsmiljøet på grunnlag av de ovennevnte prinsippene. De relevante sikkerhetskravene kan inkludere enhver kombinasjon av tekniske og organisatoriske tiltak som påvirker IT-sikkerheten til driftsmiljøet til det medisinske utstyret.

Eksempler på uønskede hendelser av betydning for informasjonssikkerhet knyttet til medisinsk utstyr

Disse eksemplene kan brukes som utgangspunkt for risikovurdering. Listen over uønskede hendelser må tilpasses virksomheten.

1. Ansatte har ikke fått opplæring i hvordan bruk av MU skal skje i henhold til rutiner i virksomheten.
2. Pasient ser opplysninger om en annen pasient på PC/visningsutstyr (som er plassert slik at innsyn er mulig).
3. Manglende passord/felles passord på utstyret.
4. MU/Server med helse- og personopplysninger fra MU er stjålet (inklusive sikkerhetskopi som satt i maskinen).
5. Identifiserbare helse- og personopplysninger på MU som ikke lenger er nødvendige og relevante blir ikke slettet.
6. Manglende tilgangskontroll til utstyr, system eller lagringsområde med helse- og personopplysninger (personell uten tjenstlig behov har tilgang).
7. Manglende hendelsesregistrering hos utstyr, system eller lagringsområde med helse- og personopplysninger.
8. Ansatt som slutter blir ikke fjernet som bruker i system med tilgang til helse- og personopplysninger fra MU.
9. Helse- og personopplysninger fra MU inkluderes ikke i backup.
10. Manglende tilgjengelighet ved lokale systemfeil.
11. Manglende tilgjengelighet ved nedetid på sentral infrastruktur.
12. Sikkerhetskopi oppbevares ikke avlåst, brannsikkert og adskilt fra driftsutstyret.
13. Digitale angrep (datavirus eller ondsinnet kode via f.eks. minnepinne eller nettverk) fører til at utstyret blir utilgjengelig.
14. Digitale angrep mot MU, slik at utstyret blir brohode for slike angrep videre inn i infrastrukturen.
15. Manglende kryptering/sikring av trådløs kommunikasjon kan medføre uautorisert tilgang til opplysninger.
16. Utilsiktet lagring av helse- og personopplysninger hos leverandør (ved fjernaksess for support).
17. Utilsiktet lagring av helse- og personopplysninger i tekniske logger.
18. Manglende databehandleravtale der det er krav til dette.
19. Data slettes ikke hos databehandler ved opphør av avtale.
20. Manglende avtaler for tjenestenivå, f.eks. oppetid og support.
21. Utlevering av personopplysninger utenfor EU/EØS-området.
22. Det lagres helse- og personopplysninger som ikke er lenger er nødvendig og relevante på utstyr/system.