INNHOLDSFORTEGNELSE

1 Definisjoner

Behandlingsansvarlig/Databehandlingsansvarlig: Den som bestemmer formålet med behandlingen av personopplysninger/helseopplysninger og hvilke hjelpemidler som skal brukes. I helseregisterloven er begrepet databehandlingsansvarlig benyttet for å unngå misforståelse med medisinsk behandling, og gjelder hvis ikke databehandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven. Se kapittel 5 for hvordan dette gjennomføres for sykehuset.

Databehandler: Den som behandler personopplysninger/helseopplysninger på vegne av behandlingsansvarlige/databehandlingsansvarlige. Dette er typisk en ekstern driftsoperatør som drifter IKT-løsninger som inneholder personopplysninger på vegne av UNN eller hvor en helsetjeneste utføres på vegne av UNN.

Behandling av helseopplysninger: Enhver formålsbestemt bruk av helseopplysninger, som f. eks innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

Behandlingsrettet helseregister: Journal- og informasjonssystem eller annet helseregister som har til formål å gi grunnlag for handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte pasient og som utføres av helsepersonell, samt administrasjon av slike handlinger.

Personopplysninger: Opplysninger og vurderinger som kan knyttes til en enkeltperson.

Sensitive personopplysninger: Opplysninger om

a) Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller relegiøs oppfatning,
b) At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
c) Helseforhold
d) Seksuelle forhold,
e) Medlemskap i fagforeninger

Helseopplysninger: Taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson.

Anonyme opplysninger: Opplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson.

Avidentifiserte helseopplysninger: Helseopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke umiddelbart kan knyttes til en enkeltperson, og hvor identitet bare kan tilbakeføres ved sammenstilling med de samme opplysninger som tidligere er fjernet. Man skal være oppmerksom på at opplysningene i seg selv, uten personentydige kjennetegn, kan være nok til å identifisere den enkelte person og anses også som avidentifiserte helseopplysninger.

Samtykke: En frivillig, utrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv.

Konsesjon: Tillatelse fra Datatilsynet til å behandle sensitive personopplysninger. Tillatelsen er gitt med vilkår i konsesjon og lov, og er begrenset til prosjektets angitte formål og sikkerhetsregulering som konsesjonen er gitt for.

Melding: Selverklæring når det gjelder behandling og sikkerhetsregulering av personopplysninger med vilkår i lov, og gir forutsetninger for behandlingen av opplysningene. Vil være grunnlag for eventuell tilsyn.

Interne: Omfatter i utgangspunktet egne ansatte som er autorisert for tilgang til UNN's nettverk.

Eksterne: Omfatter ansatte hos UNN's partnere, leverandører og databehandlere som undertegner taushetserklæring og som derved gis autorisasjon til UNN's nettverk og tjenester.

2 FORMÅL

Formålet med disse retningslinjer er å sikre at nødvendige sikkerhetsaspekter blir tatt med i avtaler med databehandler samt andre partnere og leverandører av IKT-tjenester. Retningslinjene er en del av UNN's internkontrollsystem, slik som beskrevet i helseregisterloven og personopplysningsloven.

3 OMFANG

Instruksen gjelder ved all bruk av databehandler samt andre partnere og leverandører av IKT-tjenester hvor personopplysninger vil bli eller kan bli overført til den eksterne partneren. Dette vil omfatte både full ekstern drift av tjenester, i ulik grad bruk av online-service og bruk av utvikler hvor personopplysninger/helseopplysninger overføres eller vil kunne overføres til ekstern part for drift, utvikling, prosessering eller andre tilsvarende tjenester.

4 ANSVAR

UNN ved direktøren er behandlingsansvarlig/databehandlingsansvarlig for all behandling av personopplysninger/helseopplysninger med tilknytning til UNN. Direktøren har ansvar for at alle personopplysninger blir behandlet i henhold til gjeldende lovverk, se spesielt helselovgivningen og personopplysningsloven med forskrift.

Sjef kliniske avdelinger, Sjef medisinske serviceavdelinger og Sjef almenteknisk avdelinger har det overordnede ansvar for oppfylling av disse retningslinjer i egen avdeling.

Avdelingslederen har ansvaret for oppfylling av disse retningslinjer på egen avdeling.

Ansatte som i kraft av sin stilling på UNN kan inngå avtaler med databehandler og andre partnere og leverandører av IKT-tjenester, er ansvarlig for å oppfylle disse retningslinjer. Dette innebærer ansvaret for å vurdere og detaljere punktene angitt i kapittel 6. Disse krav kan ikke fravikes. Se kapittel 6 for hvordan dette ansvaret utøves i praksis.

5 SIKKERHET I AVTALE MED DATABEHANDLER

Sikkerhetsnivået er etablert for å kunne gi et akseptabelt risikonivå for håndtering av sensitive personopplysninger, samtidig som eksterne tjenester er tilgjengelig i samme nettverk.

Ved anskaffelse av tjenester fra ekstern leverandør, skal følgende sikkerhetstiltak iverksettes:

- Leverandøren skal i sine tjenester legge til grunn UNN's sikkerhetsarkitektur
- Sikkerhetstiltak som er nødvendige for tjenesteoppdraget må avdekkes og avtales.

Anskaffelsens skal tilfredsstille til enhver tid gjeldende relevante lover, forskrifter og retningslinjer, herunder personopplysningsloven, arbeidsmiljøloven, helsepersonelloven m.v.

Kapittel 6 skal alltid vurderes i forhold til relevans i forbindelse med anbud/forespørsler ved anskaffelse av IKT-tjenester, og konklusjoner skal alltid ligge som en del av underlagsdokumentasjonen. Dersom enkelte del-kapitler ikke vurderes som relevante, skal de likevel dokumenteres i underlagsdokumentasjonen og markeres med følgende tekst: "Vurdert og ikke funnet relevant".

Relevante del-kapitler skal alltid tas med i anbud/forespørsler ved anskaffelse av IKT-tjenester, og i de avtaler som inngås. Dette skal gjøres under en felles overskrift "sikkerhet" hvor alle relevante del-kapitler som angår sikkerhetskrav samles. I praksis sikres dette ved at relevante del-kapitler fra kapittel 6:

- skal inkluderes i alle tilbuds- og anbudsdokumentene, og presiseres som absolutte krav
- skal inkluderes i bilagene til Statens standardavtale – Kjøpsavtalen (i bilag 10 for de deler som skal erstatte standardavtalen og bilag 1 for øvrige relevante deler).
- skal inkluderes i bilagene til Statens standardavtale – Vedlikeholdsavtalen (bilag 7 for de deler som skal erstatte standardavtalen og bilag 3 for øvrige relevante deler).

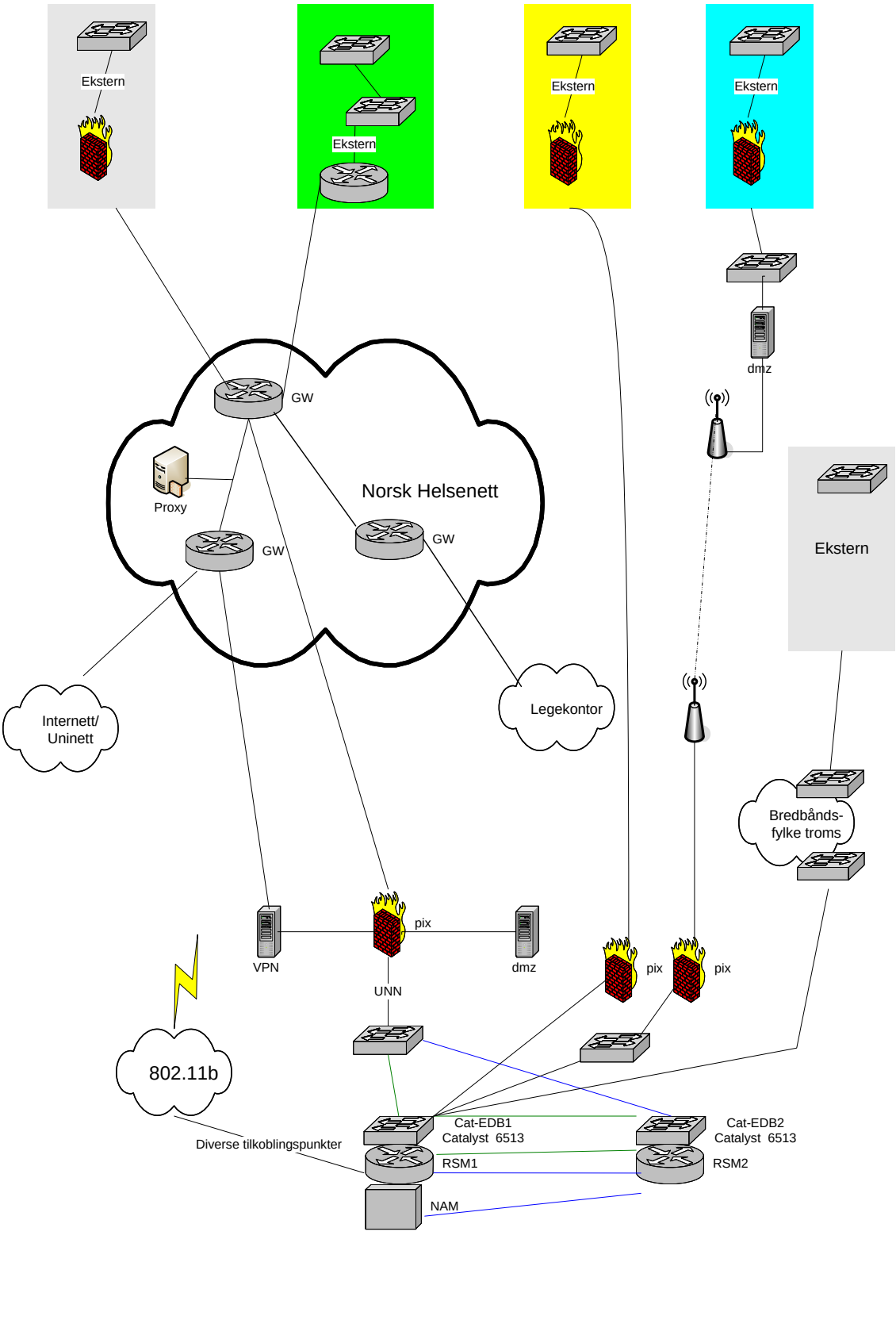
5.1 HOVEDPRINSIPPER I EKSISTERENDE SIKKERHETSARKITEKTUR

Sikkerhetsbehov omfatter følgende aspekter:

- Tilgjengelighet, dvs. sikre at informasjon og tjenester/ressurser er tilgjengelig til rett tid for det personellet som har behov for å få tilgang
- Integritet, dvs. sikre at informasjonen og tjenester/ressurser kun er tilgjengelig for autoriserte og ikke forandres av personell uten lovlig tilgang eller feil i utstyr og programvare
- Konfidensialitet, dvs sikre at informasjon beskyttes slik at innsyn fra uvedkommende hindres.

I det følgende presenteres hovedprinsipper for sikkerhetsarkitektur som må tas hensyn til ved bruk av databehandler, slik at sikkerhetsnivået opprettholdes ved slik bruk. Databehandler må i sin konfigurasjon sannsynliggjøre hvordan tilsvarende sikkerhet er etablert, se kapittel 6.3.4 og 6.3.6.

Kritiske deler av løsningen kjøres i parallelle driftsmiljøer, andre med ulik grad av reserveløsninger, for å tilfredsstille oppetid og tilgjengelighet. For tjenester som skal etableres, må det i tillegg synliggjøres slike sikkerhetsbehov, se kapitel 6.3.1.



Figur 1 Hovedprinsipper i sikkerhetsarkitektur

5.1.1 Mot eksterne

I forhold til eksterne (egne avdelinger, leverandører og partnere) må løsningene ta høyde for å motstå ondsinnede handlinger og høy kompetanse hos mulig inntrenger, slik at forsøk på å:

- Trenge inn i virksomhetens nettverk
- Sende inn ondsinnet kode som kan
    - Sende ut informasjon eller passord
    - Ta over kontrollen av de interne nettverk og derved forhindre tilgang til tjenester.

Løsningen må forhindre dette ved:

- Å ha minst 2 sikkerhetsbarrierer (ulik policy) mellom internett og områder (sikre soner) hvor sensitive personopplysninger behandles
- Begrense tjenester og protokoller til et minimum og kun etter behov
- Virussjekk av e-post og vedlegg
- Begrense muligheter for annen ondsinnet kode

6 MALER

6.1 Databehandleravtale
6.2 Kontraktmal - fjerntilgang