Hvilken rolle spiller sikkerhetspolicy for UUS?

Heidi Thorstensen
IKT-sikkerhetssjef/Personvernombud

Hva slags opplysninger håndteres?

- Sykehuset har store mengder svært sensitive personopplysninger om pasienter og deres helse
  - Pasientjournal, som viser helsehjelp gitt til enkeltpersoner over tid
  - Kvalitetsregistre, for å sikre kvalitetsforbedring i diagnostisering og behandling gitt ved sykehuset
  - Forskningsregistre, for å komme lenger i behandlingsformer og lære årsakssammenhenger innen medisinsk forskning
- Ansatteopplysninger, som også kan inneholde sensitive personopplysninger
- Andre opplysninger som kan/skal unntas offentligheten

Viktige lover som regulerer behandlingen

- Helseregisterlov med forskrifter
- Helsepersonellov
- Pasientrettighetslov
- Personopplysningslov med forskrift
- Journalforskrift
- Offentlighetslov
- med flere….

Krav til forvaltning av opplysningene

- Formål med behandlingen av personopplysninger er
  - gitt i lov/forskrift
  - konsesjoner/meldinger
- Regulerer krav til sikkerhet ved oppbevaring, tilgang, samhandling, utlevering og varighet for oppbevaring
- Regulerer krav til rettigheter for de registrerte
- Regulerer krav til dokumentasjon
- Regulerer krav til internkontroll

Hva omfatter sikkerhet?

- Konfidensialitet
  - kun autoriserte skal ha tilgang
- Tilgjengelighet
  - autorisert personell skal ha tilgang til korrekte ressurser og informasjon til rett tid og riktig tidsomfang
- Integritet
  - informasjonen skal til enhver tid være resultat av rettmessige registreringer og kontrollerte aktiviteter
- Kvalitet
  - informasjonen skal til enhver tid være fullstendig, oppdatert og korrekt.

Hvor er de elektroniske opplysninger?

- Elektronisk journal og pasientadministrativt system
- Spesialistmoduler som egne eller tilknyttede elektroniske applikasjoner
- Medisinsk teknisk utstyr, eks
  - EKG og EEG
  - Røntgen
  - Lab-system
  - Økende grad av elektroniske prøvetakinger: "Gastro-pille" – elektronisk bildetaking i tarmene
- Kreves i økende grad elektronisk formidlet til andre – andre sykehus, primærhelsetjenesten, meldinger til RTV, SSB, med flere

Styringssystem for sikkerhet

- Ledelse
- Organisasjon og ansvar
- Tiltak
- Andre virksomheter
- Oppfølging
- Dokumentasjon

Styringssystem for sikkerhet

- Ledelse
  - Sikkerhetsmål
  - Sikkerhetsstrategi
  - Akseptabelt risikonivå
    - sikkerhetsbrudd aksepteres ikke
    - iverksetter sikkerhetstiltak for å begrense risiko knyttet til behandling av personopplysninger
    - benytter risikovurdering for å etablere sikkerhetsnivå og ved endringer
    - økonomi er ikke et argument for lavere sikkerhet – kan ikke bruke økonomi som måleinstrument
- Organisasjon og ansvar
  - Sikkerhetsorganisering og ansvar
  - Sikkerhetsinstruks

Styringssystem for sikkerhet

- Sikkerhetstiltak
  - Taushetsplikt og opplæring
  - Autorisasjon og tilgang
  - Beredskapshåndtering
  - Etablering av sikkerhetstiltak iht det som er avdekket ved risikovurderinger
- Avtale med andre virksomheter
  - Sikre nødvendig sikkerhetsnivå
  - Sikre bruk/behandling av personopplysninger
  - Sikre oppfølgingsrett for ansvarlig virksomhet

Styringssystem for sikkerhet

- Oppfølging
  - Revisjoner
  - Konfigurasjonsoversikt og endringshåndtering
  - Avviksbehandling
  - Ledelsens gjennomgang av avdekkede behov og avvik – grunnlag for eventuell endring i sikkerhetsmål og -strategi
- Dokumentasjon
  - Oversikt over behandling av personopplysninger
  - Logging
  - Dokumentasjon og oppbevaringsplikt

Styringssystem for sikkerhet – hvilken rolle for UUS

- Nødvendig for å
  - håndtere sikkerhetsbehov og -krav i stadig mer komplekse løsninger
  - overholde lovverket
    - Skal ha et styringssystem for sikkerhet
    - Skal sikre tilstrekkelig sikkerhet ved all behandling av personopplysninger (konfidensialitet, tilgjengelig, integritet og kvalitet)
    - Skal sikre rettigheter til den registrerte
  - samhandle med andre, hver juridiske virksomhet (HF og RHF) er selvstendig ansvarlig
    - Krav om at virksomheten må forsikre seg om at mottaker av elektroniske opplysninger har tilstrekkelig sikkerhet
    - Kunne avtale løsninger mellom parter som kommuniserer
    - Kunne sikre tilstrekkelig sikkerhet ved bruk av partnere/leverandører
    - Kunne kontrollere partnere/leverandører

Etablering av felles Styringssystem for sikkerhet – regionalt og nasjonalt

- Krav om mer elektronisk samhandling – behandlingskjeden av pasienter på tvers av Helseforetak og fritt sykehusvalg
  - Nå må alle parter forsikre seg om hverandres sikkerhetsnivå
  - Ansvaret ligger på hver juridiske enhet
- Krav om bruk av Norsk Helsenett (NHN)
  - Skal NHN måtte sikkerhetsmessige vurdere alle aktører?
  - Hvordan formidle dette tilfredsstillende til alle aktørene?
- Nasjonale initiativ for samhandlende løsninger
  - Hvem og hvordan skal alle parter forsikre seg om hverandres sikkerhetsnivå?

➢ Pågår arbeid med å etablere **Felles styringssystem for sikkerhet** innen spesialisthelsetjenesten, for å muliggjøre den stadig sterkere forventningen om og behovet for samhandling