JurPreM

Problemstilling:

Kan pasienten samtykke til «dårligere» informasjonssikkerhet?

a. Problemstillingen er sendt inn fra medisinsk genetikk v/Dag Erik Undlien (OUS): Informert samtykke kan brukes i forskning (og i helsetjenesten) til å inkludere pasienter i prosjekter som innebærer en viss risiko for pasientene. Kan samtykke også benyttes til å utsette seg for personvernrisiko» gjennom å si ja til å benytte IKT-løsninger som ikke tilfredsstiller alle krav til IKT[1]sikkerhet og personvern?

Mitt inntrykk er at dette per i dag praktiseres på en måte som tilsier at kravene til ivaretagelse av personvern og IKT-løsninger nærmest er absolutte og noe man ikke kan samtykke seg bort fra. Et konkret eksempel hos oss fra noen år tilbake var da våre leger ønsket å teste ut et program for ansiktsgjenkjenning («face to gene») til bruk ved diagnostikk av sjeldne arvelige sykdommer. Programmet kjørte i skyen og tilfredsstilte ikke alle krav til en IKT[1]løsning for håndtering av sensitive data ved vårt sykehus. Vi ble forklart at dette kunne man ikke samtykke seg bort fra (vi er rimelig sikre på at flere pasienter ville ha sagt ja til å benytte dette tilbudet i jakt på en diagnose til tross for en viss personvernrisiko).

Kan man samtykke til dårligere personvern?

Personvernforordningen (GDPR) omhandler virksomheters behandling av personopplysninger og gjelder for all behandling av personopplysninger. GDPR artikkel 5 og artikkel 32 omhandler informasjonssikkerhet.

Artikkel 5 bokstav f fastsetter at personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet, inkludert beskyttelse mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved at dataansvarlig må ta i bruk passende tekniske eller organisatoriske tiltak.

Dette betyr at det alltid må være et grunnleggende nivå av sikkerhet for personopplysninger, uavhengig av samtykke. Å samtykke til dårligere sikkerhet ville bryte med dette prinsippet om integritet og konfidensialitet.

Artikkel 32 spesifiserer at behandlingsansvarlige og databehandlere må implementere passende tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er passende i forhold til risikoen. Dette inkluderer tiltak som pseudonymisering og kryptering av personopplysninger, samt evnen til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene

Det å tillate dårligere sikkerhet gjennom samtykke vil undergrave disse kravene og sette personopplysningene i fare.

Sammen sikrer disse artiklene at det alltid må være et minimumsnivå av sikkerhet og beskyttelse for personopplysninger. Selv om en person gir samtykke, kan ikke dette samtykket brukes til å omgå de grunnleggende sikkerhetskravene som er fastsatt i GDPR. Dette beskytter individers rettigheter og friheter, og sikrer at personopplysninger behandles på en sikker og ansvarlig måte. Det er dataansvarlige som er pliktsubjektet og som er ansvarlig for overholdelse av GDPR.