SIKKER PASIENTJOURNAL?

MARIA LILLEMOEN
INFORMASJONSRÅDGIVER VED HØGSKOLEN I GJØVIK

Helsesektoren har som resten av samfunnet gjennomgått en elektronisk revolusjon de siste årene. Spesielt for helsesektoren er at medisinske journaler utgjør et svært komplekst system med et stort antall brukere og sensitiv medisinsk informasjon.

I juni i 2009 ble Helseregisterloven endret, og åpner blant annet for å etablere behandlingsrettede helseregistre på tvers av juridiske enheter i helsetjenesten. Men dette er omdiskutert. Noen mener at en felles nasjonal database med pasientjournaler er veien å gå, mens andre er svært kritiske til dette, blant annet Datatilsynet. For hva med sikkerheten? En nasjonal database med pasientjournaler vil kunne redde liv, men det er også en høyere risiko for at sensitive opplysninger kan komme på avveie. Et slikt system krever streng sikring, der tilgangskontroll og autentisering blir svært viktig. Autentisering er verifikasjon av påstått identitet og dette bruker vi hver dag for eksempel ved å logge inn på pc-en og i ulike programmer og databaser.

Førsteamanuensis Kirsi Helkala ved Høgskolen i Gjøvik har skrevet doktorgradsavhandling som tar for seg autentisering i helsesektoren. Innen denne sektoren er det kanskje ekstra viktig at sikkerheten i disse autentiseringsmetodene er best mulig slik at ingen uvedkommende kan logge seg inn og se for eksempel journaler. Det finnes tre hovedkategorier av autentiseringsmekanismer. Disse karakteriseres av noe en bruker vet, bruker eller er. For eksempel passord, smartkort eller fingeravtrykk. Helkala har kartlagt bruken, identifisert mulige forbedringer for å utvikle nye eller forbedre eksisterende mekanismer for autentisering.

Det som er mest brukt i helseforetaket Helkala undersøkte, er å bruke passord for å logge inn i de ulike systemene. Det kan gjerne være store utfordringer ved å bruke passordbasert autentisering. Ofte er det dårlig kvalitet på brukergenererte passord, noe som både kan ligge til brukeren eller at kriteriene for passord som er definert i systemene er for generelle. Dette gjelder da ikke bare for passord i helseforetakene, det gjelder for mange institusjoner og bedrifter. I forskningen sin har Helkala lagd et verktøy for å måle passordkvalitet. Dette viser seg å være et svært nyttig hjelpemiddel når passord skal genereres. Det viser seg også at brukere trenger opplæring i gode passordrutiner, systemene må sette krav, ellers vil brukere ta den letteste veien når de lager passord.

Men hvis vi ikke lager gode nok passord, hva skal vi bruke da? Effektivitet og sikkerhet er viktig her. I avhandlingen har Helkala utarbeidet en rangeringsmetode som kan brukes når nye produkter velges. Det viktige når nye produkter velges, er at produktene passer best mulig til brukerne og brukermiljøene, ikke bare at det er sikkert eller billig.

Flere leger tar notater under konsultasjoner ved å benytte et program som skriver ned teksten man leser inn på diktafon eller lignende. Da vil det være naturlig å bruke autentiseringsprodukter som er basert på stemmeverifisering. Å lese av håndavtrykk kan også brukes som autentiseringsmetode for å få tilgang til ulike

områder. Dette brukes den dag i dag i fornøyelsesparker, men innen helsetjenestene ville dette være regnet som lite hygienisk. Begge er eksempler hvor brukeren ikke trenger å utføre ekstra arbeid eller gå inn i et ukjent brukergrensesnitt for å autentisere seg. For hvis autentiseringsproduktet fungerer som det skal, vil også den ordentlige jobben bli gjort fortere. Andre aktuelle metoder for bruk i helsevesenet vil være autentisering ved hjelp av ganglag eller ansiktsgjenkjennelse.

En nasjonal database med pasientjournaler setter svært strenge krav til sikkerheten, og når og om en slik database blir en realitet er usikkert. Det som er helt sikkert er at det også blir særdeles viktig å ta hensyn til brukergruppen når slike systemer blir utformet. Blir terskelen for brukerne for høy, vil heller ikke systemene bli brukt.