DATASIKKERHET *på legekontor*

AV EVA HENRIKSEN / EVA SKIPENES
NST – Nasjonalt Senter for Telemedisin, Tromsø

DAG NORDVÅG
Sentrum Legekontor, Tromsø

Denne artikkelen er for en stor del basert på et prosjekt som ble gjennomført våren 2003 i regi av Nasjonalt senter for telemedisin (NST) og Sentrum legekontor i Tromsø.

Bakgrunnen for prosjektet var ny personvernlovgivning gjeldende fra 1. januar 2001 (med overgangsordning til 1. januar 2003), og dens implikasjoner for elektroniske pasientjournaler (EPJ) og informasjons- og kommunikasjonssystemet som sådan. Helsenettilkobling med mulighet for internettaksess og elektronisk post på samme datamaskin som EPJ nødvendiggjør innsats på området, også på de minste legekontor.

Virksomheter i helsesektoren har nå meldeplikt til datatilsynet for all elektronisk behandling av personopplysninger, dvs EPJ-system og elektronisk kommunikasjon (www.datatilsynet.no under menyen «Melding og konsesjon»). Meldingen skal bekrefte at legekontoret har sikkerhetsdokumentasjon, har utført risikoanalyse og har utarbeidet opplegg for systemrevisjoner, vedlikehold og versjonskontroll. I praksis faller dette ansvar på den dataansvarlige i virksomheten, men det formelle ansvaret ligger hos ledelsen (styreleder eller ansvarlig eier) eller hos den enkelte lege i kontorfellesskap uten daglig leder. Datatilsynets kontroller av virksomheter i helsevesenet i 2002 avdekket vesentlige mangler på disse punkt (http://hetti.datatilsynet.no/espor/2002/6/spor.html). Ytterligere kontroll av legekontor og sykehus forventes i tiden fremover.

For Nasjonalt senter for telemedisin sin del var målet for prosjektet å bidra til å etablere/ revidere overnevnte system på et legekontor for derved å lage en mal for tilsvarende arbeid andre steder. Arbeidet ble gjort med basis i gjeldende lovverk og med bakgrunn i veiledninger for arbeidet med informasjonssikkerhet utgitt av:

- Datatilsynet (www.datatilsynet.no/dtweb/attachment/780/Risikovurdering_TV-506_02.pdf)
- SHDir (www.shdir.no/index.db2?id=2192)
- KITH (www.kith.no/vedlegg/11405/rosmet.pdf)

Prosjektet reetablerte for Sentrum legekontors del dokumentasjon på informasjons- og kommunikasjonssystemet, med styringssystem, risikoanalyse og dokumentasjon av praktiske prosedyrer inklusive avvik. I tillegg ble det avdekket et par svakheter, av moderat alvorlighet, i systemene til leverandører. Disse ble korrigert underveis.
Prosjektet ble avsluttet sommeren 2003.

Lovpålagte bestemmelser

De mest relevante lover og forskrifter i denne sammenheng er

- helseregisterloven (http://www.lovdata.no/all/nl-20010518-024.html)
- personopplysningsloven (http://www.lovdata.no/all/nl-20000414-031.html)
- forskriften til personopplysningsloven (http://www.lovdata.no/for/sf/aa/aa-20001215-1265.html)

Lover som er mer spesialiserte har presedens foran lover av mer generell karakter, f.eks. går helseregisterloven foran personopplysningsloven. Et viktig anliggende i disse lovene er at informasjonssikkerheten skal hjelpe helsepersonell til å ivareta taushetsplikten og hindre utilsiktet endring av pasientinformasjon. Et annet viktig anliggende er at aktuelle opplysninger skal være tilgjengelige slik at det kan ytes nødvendig helsehjelp.

Helseregisterloven og personopplysningsloven stiller likelydende krav til informasjons-sikkerhet (med unntak av at helseregisterloven har et tillegg om kvalitet). Ett av kravene er at virksomhetene gjennom planlagte og systematiske til-

Dag Nordvåg i arbeid foran pc'en på legekontoret

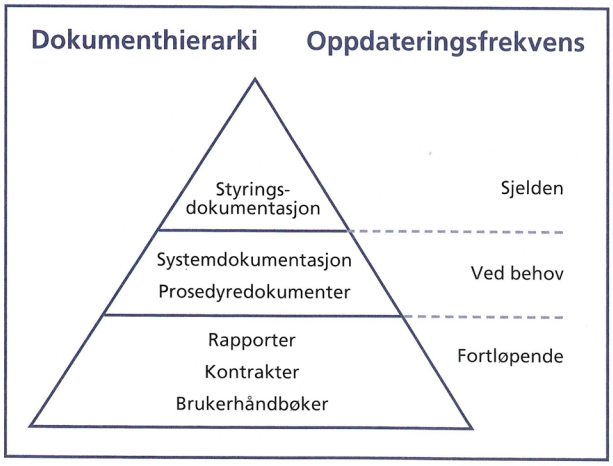
tak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. For å oppnå en slik tilfredsstillende sikkerhet skal informasjonssystemet og sikkerhetstiltakene dokumenteres. [Helseregisterloven §16, Personopplysningsloven §13].

I forskriften og lovene stilles det også krav om at den enkelte virksomhet (ved daglig leder eller tilsvarende) skal etablere et internt styringssystem for informasjonssikkerhet, og ha rutiner for jevnlig sikkerhetsrevisjon. [Helseregisterloven §17, Personopplysningsloven §14, Personopplysningsforskriften §§ 2–3 og 2–16].

En forutsetning for å kunne ivareta informasjonssikkerheten er at den dataansvarlige og medarbeiderne har nødvendig kompetanse til å bruke informasjonssystemet. Ledelsen skal sørge for at denne kompetansen tilegnes og vedlikeholdes. [Personopplysningsforskriften §2–8].

Styringssystem for informasjonssikkerhet

For å oppfylle de lovpålagte kravene om å ha planlagte og systematiske tiltak for å ivareta informasjonssikkerheten, anbefales det at man etablerer et styringssystem for informasjons-sikkerhet. Et slikt styringssystem skal omfatte dokumentasjon av informasjonssystemet, inkludert mål, strategi og retningslinjer for informasjonssikkerhet. Tiltak for å ivareta informasjonssikkerheten må beskrives. Disse tiltakene omfatter både tekniske og programmessige installasjoner i tillegg til organisatoriske rutiner og prosedyrer. Styringssystemet kan illustreres som et hierarkisk system, som vist i figuren under.



Et styringssystem består av flere typer dokumenter; eventuelt kan de ulike dokumentene inngå som deler av et felles dokument. Et forslag til hvilke dokumenter som bør omfattes av styringssystemet blir vist på neste side.

	Dokumentnavn	Beskrivelse
Styringsdokumentasjon	Overordnet styringsdokument	Skal inneholde beskrivelse av de beslutninger som ligger til grunn for sikkerhetsarbeidet – dvs beskrivelse av sikkerhetsmål og sikkerhetsstrategi. Ansvar og myndighet knyttet til sikkerhetsarbeidet skal også beskrives.
Systemdokumentasjon og prosedyredokumenter Prosedyredokumenter	Systemdokumentasjon	En overordnet beskrivelse av datasystemet, med nettskisser.
	Retningslinjer for bruk av datasystemene ved legekontoret	Krav til de ansattes bruk av datasystemene.
	Prosedyre for sikkerhetskopiering (backup)	Hvem utfører, hvor ofte, lagring, testing, etc.
	Prosedyre for avviksbehandling	Hva er avvik, hvordan rapporteres avvik, oppfølging, ansvar.
	Prosedyre for sikkerhetsrevisjon	Rutinemessig gjennomgang av om sikkerhetstiltakene fungerer etter mål og hensikt.
	Prosedyre for forebyggende systemvedlikehold (inkludert sikkerhet)	Beskrive oppgaver som er nødvendig for å kunne ha et stabilt og sikkert driftsmiljø for datasystemet.
	Prosedyre for intern opplæring	Hva skal opplæringen omfatte, hvem skal få opplæring, hvor ofte.
Rapporter og andre dokumenter	Risikovurdering(er)	(Se neste avsnitt)
	Referat fra sikkerhetsrevisjon	(Se beskrivelse under prosedyredokumenter)
	Rapporter fra avviksbehandling	Rapporter om avvik og iverksatte tiltak
	Kontrakter med underleverandører	
	Brukerhåndbøker	
	Interne installasjonsveiledere	
	Nødvendige spesifikasjoner av systeminnstillinger	
	Signaturlister for gjennomført brukeropplæring	

Beskrivelse av NSTs utkast til styrings-system for legekontor finnes på internett: http://www.telemed.no/cparticle84896-4259.html. På denne adressen finnes også nedlastbare dokumenter (i MS Word format) som kan benyttes som eksempler/maler for oppbygging av et slikt styringssystem.

Gjennomføring av risikovurdering

Som en viktig del av arbeidet med informasjonssikkerhet er helseforetak og andre institusjoner som behandler personopplysninger gjennom personopplysningsforskriften pålagt å gjennomføre risikovurdering. [Personopplysningsforskriften §2–4]

Vi vil her gi en kort oppsummering av hvordan dette kan gjøres. Målet for risikovurderingen er å avdekke det sikkerhets-messige risikonivået ved legekontorets informasjonssystem (inkludert ekstern kommunikasjon) og foreslå eventuelle tiltak for å redusere risikonivået.

Gangen i en risikovurdering

- Beskrive mål og omfang av risikovurderingen.
- Kartlegge trusler, sårbarheter og uønskede hendelser
- Trusselanalyse: vurdere sannsynlighet og konsekvens for de identifiserte truslene
- Beregne risikonivå
- Foreslå tiltak for å redusere risikonivået

En *beskrivelse av mål og omfang* av risikoanalysen forutsetter dokumentasjon av system og omgivelser. Dette kan dekkes av dokumentasjonen som inngår i styringssystemet. Den bør vise en skisse av datasystemet og nettverket (lokalt og eksternt), beskrive programvare som er i bruk, eksisterende sikkerhetstiltak (brannmurer, passordrutiner, fysisk sikring, backup-rutiner, etc), akseptabelt risikonivå, og lovpålagte krav til informasjonssikkerhet. *Ved kartlegging av trusler* er det viktig å tenke på ulike kategorier av trusler. En måte å kategorisere truslene på er følgende:

- Trusler utenfra (fra eksterne nett)
- Trusler innenfra (lokalt på legekontoret)
- Trusler «ovenfra» (strømbrudd, brann, oversvømmelse etc)

For hver av de tre kategoriene over:
- Tilsiktede trusler
- Utilsiktede trusler

Det er også viktig å identifisere sårbarheter i system og organisatoriske rutiner og prosedyrer.

Trusselanalyse innebærer å vurdere konsekvens og sannsynlighet for hver av de identifiserte truslene. Konsekvens bør vurderes både i forhold til personvern, liv og helse, økonomi og anseelse. Sannsynlighet vil være relatert til kjente sårbarheter, og kan beskrives i form av frekvens, gjerne basert på historiske data eller erfaringer. Det anbefales å benytte tre til fem nivå for både konsekvens og sannsynlighet, og de ulike nivåene må være definert på forhånd.

Risikonivået fremkommer som et produkt av konsekvens og sannsynlighet for hver trussel. Dette kan illustreres i en risikomatrise hvor konsekvens og sannsynlighet utgjør de to dimensjonene. Hver kombinasjon av konsekvens og sannsynlighet (dvs. hver celle i matrisa) må tildeles et gitt risikonivå. Risikonivåene kan illustreres med ulike farger, men må i tillegg defineres. Eksempel på dette er illustrert i følgende figur.

Konsekvens / Sannsynlighet	Liten	Moderat	Stor	Katastrofal
Nesten aldri	Lav	Lav	Lav	Moderat
Sjelden	Lav	Lav	Moderat	Høy
Ofte	Lav	Moderat	Høy	Høy
Svært ofte	Moderat	Høy	Høy	Høy

Definisjonen av risikonivå for de ulike cellene i matrisa (Høy–Moderat–Lav) må ses i sammenheng med kriteriene for akseptabelt risikonivå slik de ble beskrevet i starten av risikoanalysen, f.eks hva man gjør med trusler som havner i kategorien «Høy».

Matrisa illustrerer altså hvilke trusler som er akseptable og hvilke som er utakseptable.

Trusler som har et uakseptabelt risikonivå må det iverksettes tiltak mot. *Tiltakene* må beskrives, ansvaret for gjennomføring må plasseres (navngitt person), og frist for gjennomføring må gis. Trusler med lavere risikonivå bør også holdes under oppsyn videre, og der det er hensiktsmessig kan det også for disse iverksettes tiltak.

Oppfølging

Ved endringer som kan ha betydning for informasjonssikkerheten skal det gjennomføres ny risikoanalyse.

Sikkerhetsarbeidet skal jevnlig etterprøves for å verifisere at de sikkerhetstiltak som er besluttet etablert, faktisk er iverksatt og fungerer etter sin hensikt. Ved sikkerhetsrevisjonen skal den faktiske bruk av informasjonssystemet sammenlignes med de retningslinjer for bruk som er besluttet. [Personopplysningsforskriften §2–5]

Alle sikkerhetsbrudd, og all bruk av informasjonssystemet som er i strid med fastlagte rutiner, er avvik og skal registreres og behandles. Dersom avviket har medført uautorisert utlevering av personopplysninger, og dermed brudd på taushetsplikten, skal hendelsen rapporteres til Datatilsynet [Personopplysningsforskriften §2–6].

Referanser til relevante hjelpemidler

I regi av KUP (kvalitetsutvalg Aplf/NSAM), kvalitetsforbedringsutvalget i PSL og Infobruk og med økonomisk støtte fra DnLf og SHDir, blir det utviklet et pc-verktøy («TrinnVis») for små legepraksiser til hjelp ved etablering av et styringssystem for informasjonssikkerhet. Verktøyet har også støtte for gjennomføring av risikovurdering. Planen er å distribuere verktøyet vederlagsfritt til alle medlemmer av DnLf våren 2004.

Sosial- og Helsedirektoratet (SHDir) har startet et prosjekt for å utarbeide en bransjenorm for informasjonssikkerhet for helsesektoren. Bransjenormen tar mål av seg til å angi mer konkrete krav til sikkerhet for virksomheter som vil knytte seg til (det nasjonale) helsenettet enn det helseregisterloven, personopplysningsloven og personopplysningsforskriften gir. Alle som vil knytte seg til helsenettet må oppfylle bransjenormen. Bransjenormen skal etter planen være ferdig våren 2004.

Ulike kommersielle aktører tilbyr også verktøy for etablering av styringssystem for informasjons-sikkerhet og gjennomføring av risikovurdering. Noen av disse aktørene tilbyr konsulenthjelp ved gjennomføringen. Et eksempel på dette er firmaet DigitalHelse som tilbyr systemet RiskManager, se www.digitalhelse.com/default.asp?page=2020,2021&lang=1
KITH (Kompetanse-senteret for IT i Helsevesenet) har utarbeidet flere nyttige dokumenter som omhandler sikkerhet og risikovurdering, se bl.a
- www.kith.no/informasjonssikkerhet_virsomhetsomrade/13378/
- www.kith.no/informasjonssikkerhet_anbefalingveiledning/13509/