Datatilsynet

Sosial- og helsedirektoratet
Avdeling for IT-strategi og statistikk
Pb 7000 St Olavs plass
0130 OSLO

Deres ref.	Vår ref. (bes oppgitt ved svar)	Dato
03/2178	2005/133-2 CLU/-	29.04.2005

NORM FOR INFORMASJONSSIKKERHET I HELSESEKTOREN – DATATILSYNETS HØRINGSUTTALELSE

Det vises til brev av 18.01.2005. Vedlagt følger Datatilsynets høringsuttalelse til Norm for informasjonssikkerhet i helsesektoren.

1. Innledning

Datatilsynet mener at en god bransjenorm er et viktig hjelpemidler for godt personvern. Datatilsynet er svært positiv til at direktoratet har tar initiativet til å utarbeide en bransjenorm. Normen gir bransjens representanter et nyttig redskap i arbeidet med å tolke og implementere et lovverk som er omfattende og til dels vanskelig tilgjengelig, og er et godt supplement til loven. Forhåpentligvis vil normen kunne bidra til ensartet praksis i bransjen.

I det følgende vil Datatilsynet gi sine synspunkter på den utarbeidede bransjenormen. Først gis det noen generelle tilbakemeldinger, særlig knyttet til normens oppbygging og utforming. Deretter drøftes normens håndtering av internkontrollplikten etter helseregisterlovens § 17, jf personopplysningslovens § 14 før det gis mer konkrete kommentarer til de enkelte bestemmelsene. Avslutningsvis vil Datatilsynet kommentere bruken av faktaark og disses nærmere innhold, før hovedpunktene i høringsuttalelsen oppsummeres.

2. Generelle merknader

Normen er ment å skulle regulere enkelte av de pliktene databehandlingsansvarlige har i medhold av helseregisterloven og personopplysningsloven, primært knyttet til informasjonssikkerhet. Selv om normen er hensiktsmessig avgrenset i så måte, bør man også informere mer konkret om at databehandlingsansvarlige har en rekke andre plikter i henhold til helseregisterloven/personopplysningsloven, uten at disse faller inn under denne bransjenormens virkeområde. Datatilsynet mener en klarere avgrensning er viktig for at bransjen skal danne seg et helhetlig bilde av de aktuelle lovmessige krav. Datatilsynet ser at dette til en viss grad gjøres under punkt 3.2, men mener en regulering her kan være egnet til å forvirre leseren hvis man ikke tidligere har forklart sammenhengen. Det vises for øvrig til det som er sagt under punkt 3 når det gjelder plikten til å utarbeide et system for internkontroll.

Som nevnt i høringsbrevet, inneholder selve normen kun de kravene som må være oppfylt for å oppnå tilfredstilende informasjonssikkerhet men ingen konkret veiledning for hvordan kravene skal oppnås. Dette vil ivaretas gjennom faktaarkene. I utgangspunktet mener Datatilsynet at dette er en grei inndeling. Vi ser imidlertid enkelte problemer knyttet til at normen, men ikke faktaarkene er juridisk bindende (for de grupper dette er aktuelt for). Situasjonen blir således at deler av bransjen er bundet av en norm som ikke gir noen konkrete pålegg knyttet til tolkning av lovens/forskriftens bestemmelser. Man står dermed i fare for at normens intensjon blir vesentlig uthult i den stund normen selv bare gir en gjengivelse av lov-/forskriftsbestemmelser.

Når det gjelder spørsmålet om hvorvidt lov-/forskriftsteksten bør tas direkte inn i normen, mener Datatilsynet at den utformingen som er valgt per i dag er hensiktsmessig. Det vises særlig til at normens målgruppe, som hovedregel, ikke har juridisk bakgrunn, og således liten erfaring med å lese lovbestemmelser. Slik Datatilsynet ser det, vil gjengivelse av lovteksten bare gjøre normen mindre egnet som et nyttig oppslagsverk. Man vil i tillegg være bundet til forskriftens rekkefølge hva gjelder beskrivelse av de enkelte plikter, noe som vil kunne få uheldige konsekvenser rent pedagogisk sett. Etter tilsynets oppfatning vil kryssreferansetabellen fungere tilfredstillende for de som måtte ha særlig interesse i å fordype seg i selv lovgrunnlaget. Dersom det skal utarbeides en elektronisk versjon, anbefaler imidlertid Datatilsynet at direktoratet vurderer å legge inn en fortløpende kobling til de enkelte paragrafer.

Det presiseres i høringsbrevet at normen i enkelte tilfeller innskjerper lovverkets krav. Dette ser Datatilsynet selvfølgelig positivt på, men vi vil minne om at helseregisterloven/personopplysningsloven implementerer et EU direktiv hvis formål er å lette samhandling ved behandling av helseopplysninger/personopplysninger. Strengere regler i Norge vil således kunne vanskeliggjøre overføring av personopplysninger til andre EU/EØS-land.

3. Regulering av Internkontrollplikten

Normen omtaler bestemmelsene om internkontroll i helseregisterlovens § 17 (og personopplysningslovens § 14) en rekke steder. Det sies innledningsvis (1.2) at normen vil gi et bidrag til etterlevelse av den generelle internkontrollplikten. Styringssystemet for informasjonssikkerhet er en viktig del av en virksomhets internkontroll, men den generelle internkontrollplikten omfatter mer enn dette; internkontrollen skal sørge for at den databehandlingsansvarlige er i stand til å ivareta de plikter som den aktuelle behandlingen medfører.

Normen dekker deler av den generelle internkontrollen ved å tilkjennegi oversikten som fremstilles i personopplysningsforskriftens 3. kapittel over plikter som det skal etableres rutiner for. Sentrale deler av internkontrollen inngår som en del av sikkerhetsdokumentasjonen, eksempelvis oversikten over de ulike behandlinger. Andre deler av internkontrollen ikke nevnt. Datatilsynet er av den oppfatning at dersom normen skal omtale internkontroll, bør den samtidig gi en forståelse av hva som ligger i begrepet internkontroll, og samtidig understreke at normen ikke dekker dette i sin helhet.

Ansvar
Sentralt i forhold til regelverket er plassering av databehandlingsansvaret. Normen har databehandlingsansvarlig med i sine definisjoner (1.1). Videre omtales ansvar i kapittel 3.1 hvor dette tillegges ledelsen. Det savnes her at ansvar knyttes opp mot begrepet databehandlingsansvarlig. Videre er det, som normen beskriver, normalt at behandlingsansvaret tilligger virksomhetens ledelse. Datatilsynet opplever imidlertid at dette ofte fremstår som uklart for de små virksomheter som har valgt en organisasjonsform som ikke klart identifiserer en ledelse, og derav ikke databehandlingsansvaret. Spesielt tenkes det her på primærheletjenestens organisering med ulike enkeltmannsforetak som arbeider i et fellesskap med en form for overbygning. Datatilsynet har tidligere reist problemstillingen knyttet til organiseringen i primærhelsetjenesten og forholdet til databehandlingsansvaret i denne sammenheng ovenfor direktoratet (Datatilsynets ref. 2003/2113), uten at dette har blitt nærmere avklart. Det forventes ikke at denne problemstillingen klargjøres i normen, men det bør legges større vekt på at databehandlingsansvaret skal være klart og dokumentert, slik at de ulike virksomhetene har vurdert og dokumentert dette konkret.

Oversikt over behandlinger
I normens beskrivelse av styringsdokumenter (3.3.1 og 4.5) stilles det krav til en oversikt over de ulike behandlingene av personopplysninger. For å gi et bidrag til en generell internkontroll bør også det juridiske hjemmelsgrunnlaget for de ulike behandlingene tas med her. Videre bør dokumentasjon av behandlingsansvaret tas inn i denne sammenheng, selv om dette nok følger implisitt av kravet om organisasjons-/ansvarskart.

Normens avgrensning
Normen er i kapittel 1.5 avgrenset til å gjelde behandlinger av helse- og personopplysninger i forbindelse med pasientbehandling, herunder pasientadministrasjon og utlevering av legemidler. Andre behandlinger, som eksempelvis personaladministrasjon, er angitt til å være utenfor normens virkeområde. Slik Datatilsynet ser det faller behandlinger av person- og helseopplysninger i forskningssammenheng utenfor normens virkeområde. Dette er en viktig avgrensning for bransjen, og bør nevens eksplisitt.

Plikter etter personopplysningsforskriftens 3. kapittel
Med den avgrensingen som er gjort for normen, jf. ovenfor, vil flere av pasientens rettigheter i forhold til de registrerte opplysningen være ivaretatt av annet regelverk (helsepersonelloven, pasientrettighetsloven, journalforskriften), og det påligger ikke den databehandlingsansvarlige å dokumentere rutiner for plikter som er regulert av annet regelverk. Dette bør klargjøres i normen da omtalen i eksempelvis kapittel 5.3.3 kan gi inntrykk av at det skal utformes særskilte rutiner for slike plikter. Dersom virksomheten eksempelvis behandler helseopplysninger i forskning, vil det være krav om rutiner for blant annet innsyn i opplysningene. Dette faller imidlertid utenfor normens angitte virkeområde.

Totalt ser Datatilsynet et behov for at normen avklarer sin rolle i forhold til internkontroll. Tilsynet ser positivt på at internkontroll utover styringssystemet for informasjonssikkerhet er forsøkt tatt inn som en del av normen. Det er imidlertid viktig at det klart fremgår hva som forventes av et slikt internkontrollsystem, og hvilket bidrag normen faktisk gir til dette.

4. Kommentarer til de enkelte bestemmelsene

1.1 og 5.2.1 Om autentisering
I informasjonssikkerhetsteorien betraktes autentisering som prosessen som gjennomføres for å bekrefte en påstått identitet. For å bekrefte identiteten benyttes et eller flere autentiseringskriteria, eksempelvis et passord. Slik sett deler man ikke ut autentiseringer, men brukeridenter og autentiseringskriteria. Videre bemerkes det at 3. kulepunkt under 5.2.1 omtaler sikker tildeling av brukerident, hvor det korrekte antas å være sikker tildeling av passord.

2.1 Faktaark
Det bør foreslås en rutine som ivaretar at databehandlingsansvarlige holder seg oppdatert på nye eller endrede faktaark. Særlig ettersom det er faktaarkene som skal gi konkret veiledning på hvordan loven skal oppfylles.

3.1 Ansvar
Det bør presiseres at det *juridiske* ansvaret alltid påligger databehandlingsansvarlige selv om det daglige ansvaret delegeres.

3.3.2 Gjennomføringsdokumenter
De to øverste kulepunkt gjentar de dokumenter nevnt under styrende dokumenter (3.3.1). Slik Datatilsynet ser det hører disse hjemme under den styrende del av dokumentasjonen.

3.3.4 Lagring av logger
Hvor normen stiller krav om oppbevaring av logger i en minimumstid, bør det også understrekes at loggene, dersom oppføringen i disse kan knyttes til enkeltperson, skal slettes når formålet med loggene er oppfylt, jf personopplysningslovens § 28. Selv om loggene er et viktig hjelpemiddel for å avdekke uautorisert bruk, kan unødvendig oppbevaring av loggene medføre en personverntrussel i seg selv.

4.4.1 Akseptabel risiko med hensyn til konfidensialitet
Normens omtale av konfidensialitet kan her leses slik at den begrenses til å gjelde opplysninger som er underlagt taushetsplikt. Også opplysninger som ikke er underlagt taushetsplikten kan ha et beskyttelsesbehov med hensyn til konfidensialitet.

4.4.2, 5.3.1, 5.5.2 Omtale av blålystilgang
Generelt ser Datatilsynet på omtalen av blålystilgang eller selvautorisering som for vid. Etter Datatilsynets syn bør det i omtalen av en slik mulighet klart fremgå at kun de som har saklig behov for det, skal ha mulighet for å gjennomføre en slik selvautorisering, og at bruk av slik tilgang skal ikke bare registreres, men også følges opp konkret i hvert enkelt tilfelle.

4.5 Begrepet registeransvarlig
Normen benytter her begrepet registeransvarlig. Datatilsynet er kjent med at begrepet ofte benyttes for intern ansvarsfordelig i større institusjoner, men ser det som uheldig at det blir benyttes i normen, da det viser hen til ansvarsplasseringen etter den tidligere personregisterloven.

5.3.3 Pasientinformasjon og samtykke
Som beskrevet under ovennevnte punkt om internkontroll, er ikke dette relevante plikter etter helseregisterloven for de behandlinger av person- og helseopplysninger som normen er begrenset til å omhandle. Datatilsynet ser imidlertid at dette er nyttige understrekninger av sentrale rettigheter for pasientene, men det bør fremkomme hva som er grunnlaget for disse pliktene.

5.5.3 Klassifisering av hendelser
Normens klassifisering av hendelser kan leses som en sidestilling av konsekvensene for en pasient og konsekvensene for virksomheten på et uheldig nivå. Eksempelvis kan 2. kulepunkt ses som en sidestilling av feilbehandling av en pasient og merarbeid for personell.

5.5.3 Omtale av sikkerhetskopier
Normen omtaler test av alternativ drift og oppbevaring av sikkerhetskopier. Datatilsynet ser det som hensiktsmessig at også tilbakeføring eller annen test av sikkerhetskopier diskuteres her.

5.7.6 Kommunikasjon med pasienter og brukere
I denne sammenheng vil Datatilsynet presisere at den registrerte ikke kan samtykke seg bort fra regelverkets grunnkrav, herunder tilfredstillende informasjonssikkerhet. Lovverket er ufravikelig i så måte, og databehandlingsansvarliges plikter må følges uavhengig av hva den registrerte gis sitt samtykke til. Datatilsynet er av den grunn usikker på hva som ligger i at det må innhentes samtykke fra pasient/bruker til elektronisk formidling av helse- og personopplysninger. Generelt har Datatilsynet omtalt publikumstjenester som en akseptert nødvendighet, men at dette ikke skal være en forutsetning for å få den helsehjelpen man har krav på. Videre må man, utover å sikre tjenesten på best mulig måte, hjelpe brukeren til å ivareta sin lokale informasjonssikkerhet og sette brukeren i stand til å håndtere helseopplysningene forsvarlig.

5.8.1 Databehandlere
Hvor databehandlere omtales generelt, anbefales det at det også presiseres at forholdet til databehandlere skal reguleres i en avtale som er innskrenkende med hensyn til hva databehandler kan gjøre med person- og helseopplysningene. Databehandleren skal ikke behandle opplysningene på annen måte enn det som er avtalt med den databehandlingsansvarlige. Som omtalt i normen skal også databehandler forplikte seg til å følge sikkerhetsbestemmelsene i regelverket (her gjennom å følge normen).

6.3 Avvikshåndtering
Datatilsynet vurderer normens beskrivelse av avvik til å ha et noe høyt organisasjonsmessig nivå for håndtering av disse. I større organisasjoner bør utsjekk av avviksmeldinger og korrigerende tiltak bli iverksatt på det nivå som ledelsen har bestemt er relevant, og ikke nødvendigvis på ledelsesnivå. Hvilke avvik og hvordan avvik skal rapporteres oppover i organisasjonen avhenger av de valg virksomhetens ledelse har tatt. Det synes heller ikke hensiktsmessig at normen fastsetter at avvik skal rapporteres til nærmest leder, da den enkelte virksomhet kan velge sine rapporteringsveier. Videre er det hensiktsmessig at begrepet avvik strekkes til også å

omfatte manglende eller uhensiktsmessige rutiner, slik at rammene for behandlingene av person- og helseopplysninger til enhver tid er best mulig.

5. Kommentarer til faktaarkenes utforming og innhold

Datatilsynet har ingen kommentarer de forelagte faktaark slik de fremstår, utover at de synes å supplere normen på en god måte. For fremtidige faktaark vil Datatilsynet presisere viktigheten av at faktaarkene er så konkrete som mulig i sin angivelse av tiltak. Dette er nødvendig for at normen skal gi bransjen mer enn en oversikt over lovverkets krav.

På grunn av de ulike artene av virksomheter normen er ment å gjelde for, ses det som hensiktsmessig at faktaarkene differensieres til å passe de ulike virksomheter. Primærhelsetjenesten har typisk et annet veiledningsbehov enn hva de store helseforetakene har.

Med hensyn til hvilke faktaark som bør prioriteres, anbefaler Datatilsynet at det innledningsvis legges størst vekt på de faktaark som trengs for å oppnå tilfredstillende informasjonssikkerhet i primærhelsetjenesten, og som er hensiktsmessige for denne brukergruppen. Vi vil også fremheve viktigheten av å konkretisere kravene til tilgang og tjenstlig behov. Datatilsynets erfaring fra tilsyn, er at bransjen har store avvik i forhold til lovens krav på dette området.

Datatilsynet mener det vil være hensiktsmessig at fremtidige faktaark utarbeides i dialog med tilsynsmyndighetene, særlig ettersom disse vil inneholde mer konkrete tolkninger av lov/forskrift, hvor tilsynets praksis vil få stor betydning.

6. Oppsummering og konklusjon

Som ovennevnte høringsuttalelse viser, savner Datatilsynet primært at koblingen mellom internkontrollplikten etter helseregisterloven/personopplysningsloven generelt og den delen av internkontrollplikten som normen skal ivareta presiseres og utdypes. Det er viktig at det klart fremgår hva som forventes av et internkontrollsystem og hvilket bidrag normen er ment å gi i så måte.

For øvrig tror Datatilsynet at normen vil bli et svært godt arbeidsredskap og viktig bidrag til tilfredsstillende informasjonssikkerhet i helsesektoren.

Tilsynet ser frem til videre dialog i forbindelse med utarbeidelsen av faktaark.

Med hilsen

Georg Apenes
direktør

Christine Lie Ulrichsen
seniorrådgiver
(saksbehandler,
telefon 22 39 69 12)