DATATILSYNET

Sundhedsstyrelsen
Islands Brygge 67
2300 København S

Sendt krypteret til sst@sst.dk

17. juni 2013

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2012-621-0004
Sagsbehandler
Walther Starup-Jensen
Direkte 3319 3234

Vedrørende inspektion hos Sundhedsstyrelsen

Datatilsynet vender hermed tilbage til inspektionen, som omfattede to møder afholdt d. 30. maj 2011 og 25. oktober 2011 hos Sundhedsstyrelsen (SST) og efterfølgende korrespondance.

Disse møder har givet Datatilsynet et indblik i en komplekst område, og det er tilsynets generelle indtryk, at SST allerede arbejder med nogle af de problemstillinger, som påpeges i nærværende brev.

Efter inspektionen hos SST har Datatilsynet afholdt en inspektion hos Region Hovedstaden (Region H). Denne havde til formål at afklare, hvordan én af regionerne håndterer kommunikationen med LPR-data. Oplysninger fra inspektionen hos Region H indgår i dette brev.

Datatilsynet skal beklage den meget lange sagsbehandlingstid, som skyldes stor travlhed i tilsynet.

Fokus for inspektionen hos SST
Mødet d. 30. maj 2011 omhandlede eksterne datakommunikationsforbindelser generelt, mens mødet d. 25. oktober 2011 fokuserede på datatransmission via Sundhedsdatanettet (SDN[1]) og Sundhedsdatanettets knudepunkt (SDX[2]), hvor SST er dataansvarlig for transmissionen af persondata fra Landspatientregisteret (LPR).

Datatilsynet har fokuseret på to datatransmissioner, som fremgår af bilag 1:

- LPR-data sendt til regionerne (data om egne sygehuse og egne borgeres kontakter på sygehuse).
- Regionernes adgang til egne fejldata (fejlbehæftede data i råt format mødtet på, at regionen inkluderer data i egne it-systemer).

I den følgende tekst refereres til de typer af netværksforbindelser, som er angivet på SST's tegning i bilag 2. Af samme bilag fremgår SST's forklaring til tegningen. Når der i dette brev står "forbindelse 6" eller "forbindelsestype 6",

[1] Sundhedsdatanettet forkortes SDN eller DSDN (det Danske SundhedsDataNet).
[2] Betegnelsen SDX bruges af bl.a. MedCom til at betegne sundhedsdatanettets knudepunkt. Det bruges bl.a. i dokumenter udleveret af SST i forbindelse med inspektionerne.

er det en henvisning til den type netværksforbindelse, som har nr. 6 på tegningen i bilag 2. Nogle regioner, heriblandt Region H anvender en forbindelse af typen 6, nemlig en forbindelse der går gennem et MPLS. Andre regioner anvender den forbindelsestype, som har nr. 5 på tegningen, altså en VPN-tilslutning gennem internettet.

De firkantede parenteser angiver leverandøren.

1. SST's dataansvar og databehandlere i Sundhedsdatanettet
Til brug for mødet d. 30. maj 2011 udbad Datatilsynet sig oplysninger om, hvem der er dataansvarlig på de datatransmissioner, hvor der udveksles data med LPR. SST oplyste ved hjælp af et skema, at SST har dataansvaret for al kommunikationen over SDN for så vidt angår udveksling af oplysninger i Landspatientregisteret, hvor udvekslingen sker mellem en region og SST, dog undtaget den situation, hvor regionerne afleverer data via FTP[3] til LPR-adm.[4] hos Logica.

Denne fremstilling af dataansvaret blev ændret på mødet d. 25. oktober 2011, idet SST her oplyste, at SST ikke er dataansvarlig for den datatransmission, hvor en region henter data fra LPR-adm. hos Logica. Den nye beskrivelse af dataansvaret fremgår af de blå og røde streger på tegningen i bilag 2.

På mødet d. 30. maj udleverede SST en tegning med tilhørende forklaring, der viser to datatransmissioner fra SST til regionerne. Disse er betegnet som "LPR-data sendt til regionerne" og "Regionernes adgang til egne fejldata".

Med udgangspunkt i den sidste fremstilling (bilag 2) og tegningen udleveret på mødet d. 30. maj forstår Datatilsynet det sådan, at SST er dataansvarlig for de to transmissioner "LPR-data sendt til regionerne" og "Regionernes adgang til egne fejldata" (se bilag 1)

Ud fra det oplyste lægger Datatilsynet til grund, at SST ingen databehandleraftaler har med MedCom, Netic, Netdesign eller TDC. Af SST's forklaring til tegning i bilag 2 fremgår, at Netdesign har mulighed for at dekryptere datatrafikken, når det passerer Sundhedsdatanettets knudepunkt. TDC og Netic er angivet som underleverandører til Netdesign. Det fremgår også af forklaringen på tegningen (talebobler), at data ikke er krypteret, når de transmitteres gennem forbindelse 6, hvor TDC er angivet som leverandør.

Datatilsynet har noteret sig, at SST ved brev af 22. november 2011 har oplyst, at National Sundheds-it (NSI) har aftalt med Medcom, at der i den eksisterende tilslutningsaftale tilføjes en databehandleraftale.

---

[3] File Transfer Protocol.
[4] En web-applikation kaldet "LPR-administrationsmodulet" eller "Det LPR-administrative System". Bruges af regioner til at se deres egne data, kontakter og indberetningsfejl i Landspatientregisteret (LPR).

SST har ved brev af 22. november 2011 fremsendt en aftale indgået mellem SST og MedCom kaldet "Samarbejdsaftale om opkobling til Sundhedsdatanettets knudepunkt" underskrevet i 2004.

Vedlagt samme brev er en aftale indgået mellem NSI og MedCom, kaldet "Tilmelding til sundhedsdatanettet (SDN)". Denne aftale er indgået på et tidspunkt mellem de to møder (30. maj 2011 og 25. oktober 2011), fordi NSI her blev databehandler for SST. I aftalen angives det, at:

> *MedCom og driftsoperatøren er uden ansvar for datas eller tjenesters korrekthed, fortrolighed eller ægthed i forbindelse med brug af SDN.*

Tilsynet lægger til grund, at driftsoperatøren er én eller flere af underleverandørerne Netdesign/Netic/TDC, som er angivet på tegningen i bilag 2.

Ad. 1. - Datatilsynets vurdering
Datatilsynet har ved inspektionerne hos SST og Region H forsøgt at afklare, hvilke parter der er involveret i databehandlingen, og hvem der skal sikre et tilstrækkeligt sikkerhedsniveau ved dekryptering i SDX og ved datatransmission gennem Sundhedsdatanettet.

Den kæde af involverede parter, som er afdækket for så vidt angår Sundhedsdatanettets knudepunkt, synes at kunne beskrives således: SST anvender NSI, som anvender MedCom, som anvender NetDesign, som anvender TDC og Netic.

Dertil kommer parterne på resten af Sundhedsdatanettet.

Datatilsynet skal bemærke, at en databehandler udfører selve den praktiske behandling af personoplysninger på vegne af den dataansvarlige[5]. Tilsynet lægger til grund, at MedCom, NetDesign, Netic og TDC er SST's databehandlere. Disse virksomheder fremgår ikke af SST's seneste anmeldelse af "Landspatientregisteret" til Datatilsynet (se bilag 3).

Persondatalovens § 42, stk. 2 angiver, bl.a., at gennemførelse af en behandling ved en databehandler skal ske i henhold til en skriftlig aftale parterne imellem, og af aftalen skal det fremgå, at databehandleren alene handler efter instruks fra den dataansvarlige, og at reglerne i persondatalovens § 41, stk. 3-5, ligeledes gælder for behandlingen ved databehandleren.

SST benytter sig af én eller flere parter med adgang til ukrypterede data eller mulighed for at dekryptere data i Sundhedsdatanettetes knudepunkt. MedCom og driftsoperatøren fraskriver sig ansvar for datas eller tjenesters korrekthed, fortrolighed eller ægthed i forbindelse med brug af Sundhedsdatanettet. En sådan generel fraskrivelse af ansvar fra databehandlers side forekommer uforenelig med persondatalovens krav[6].

---

[5] Se faktaboks på denne side: http://www.datatilsynet.dk/offentlig/databehandler/
[6] Persondataloven §§ 41, stk. 3 og 42, stk. 1 og 2.

Det bemærkes i den forbindelse, at aftalen "Tilmelding til sundhedsdatanettet (SDN)", bilag 1, "Regler om brug og sikkerhed", punkt 1, angiver MedCom som ansvarlig for driften af SDN's knudepunkt.

Datatilsynet skal bemærke, at databehandlere er underlagt persondatalovens bestemmelser, uagtet den nævnte aftale underskrevet af NSI. Datatilsynet anbefaler, at SST præciserer dette overfor sine databehandlere.

SST skal endvidere sikre sig, at styrelsen har indgået databehandleraftaler, som lever op til persondatalovens § 42.[7]

SST skal endeligt sikre sig, at anmeldelser til Datatilsynet angiver alle databehandlere. Det bemærkes, at SST er ansvarlig for at anmelde eventuelle ændringer til de oplysninger, som fremgår af anmeldelser hos Datatilsynet, jf. persondatalovens § 46.

2. Sikkerheden i datatransmission fra SST til regioner via Sundhedsdatanets knudepunkt (SDX) og et MPLS-netværk (forbindelse nr. 6 på tegningen i bilag 2)

SST blev den 2. november 2011 bedt om at fremsende en redegørelse for, hvorfor SST anser MPLS-netværket[8] i forbindelse 6 for at være sikkert. I redegørelse af 22. november 2011, oplyser SST, at:

> *SST er trygge ved den sikkerhed der er i MPLS netværket på Sundhedsdatanettet. Dette begrundes i, at Sundhedsstyrelsen fra NSI har modtaget følgende vurdering af sikkerheden i mPLSnetværket, dvs. forbindelse nr. 6 på tegningen udarbejdet d. 25. oktober: "NSI betragter de mPLS baserede VPN forbindelser der anvendes på Sundhedsdatanettet for sikre, fordi de enkelte tilsluttedes trafik, på udbyderens backbone net, er separeret fra de øvrige tilsluttedes på grundlag af den fysiske destination, således at man kan betragte nettet som et lukket netværk, der sikrer at meddelelsens indhold holdes skjult for uvedkommende og at afsenders og modtagers identitet kan kontrolleres. Data som vedrører en bruger passerer ikke gennem andre brugeres netværk, så TDCs VPN mPLS net må ud fra TDCs beskrivelse betragtes som et sikkert netværk til transmission af personhenførbare ukrypterede data."*

Af bilag 2 fremgår det, at SST er dataansvarlig for en datatransmission, der går via et MPLS-netværk på forbindelse 6.

---

[7] Det bemærkes herved, at Datatilsynet ikke godkender databehandleraftaler. Umiddelbart ses de fremsendte aftaler indgået mellem SST og dennes databehandler(e) i 2004 og 2011 imidlertid ikke at indeholde det, som kræves af en databehandleraftale i medfør af persondataloven og sikkerhedsbekendtgørelsen.

[8] Et MPLS-netværk er et it-netværk, der benytter sig af Multiprotocol Label Switching. Disse netværkstyper kan laves på mange måder og sikkerheden i dem afhænger af, hvordan de er implementeret og hvordan de administreres.

SST har oplyst, at transmission af LPR-data fra SST til regionerne foregår med FTP, og at data behandles ukrypteret på Koncerndatanettet (KDN) og også i forbindelse 6 (se "talebobler" i bilag 2).

Ad. 2. - Datatilsynets vurdering
SST's redegørelse af 22. november 2011 udgøres af en henvisning til NSI's betragtning af et net kaldet *TDCs VPN mPLS net*. Af SST's redegørelse fremgår det, at NSI baserer sin betragtning på *TDC's beskrivelse*. Der er ikke redegjort for denne beskrivelse fra TDC, og det er dermed uklart, hvad der ligger til grund for, at SST anser MPLS-netværket i forbindelse 6 for at være sikkert.

SST's redegørelse angiver ikke, om NSI's betragtning af "*de mPLS baserede VPN forbindelser der anvendes på Sundhedsdatanettet*" er baseret på en reel undersøgelse af de MPLS-netværk, der anvendes i Sundhedsdatanettet.

Datatilsynet finder, at SST som dataansvarlig skal sikre sig, at der foretages en sikkerhedsmæssig vurdering af alle de datatransmissioner, som SST er dataansvarlig for.

3. Sikkerhed ved datatransmission via Sundhedsdatanettet
NSI har på vegne af SST forespurgt MedCom om, hvordan SST's trafik er adskilt fra andre kunders data. MedCom har overfor NSI fremlagt notatet "Aftalesystemet - Notat om Sundhedsdatanettets sikkerhedsmodel". Notatet indeholder forklaring af aftalesystemet samt en beskrivelse af datatransmissionen gennem Sundhedsdatanettet. Af MedComs notat fremgår det blandt andet, at:

> *Transmission af data er sikret imod uvedkommendes kendskab ved enten kryptering (3DES/AES-256) eller ved anvendelse af faste forbindelser eller MPLS-separering af data, der af Datatilsynet er sidestillet med sikkerheden på faste forbindelser i skrivelse til TDC J.nr.2002-711-0028 dateret 21. juni 2002.*

En lignende formulering fremgår af MedComs hjemmeside[9]. SST henviste også til denne hjemmesidetekst på mødet d. 25. oktober 2011.

Af referat fra mødet d. 25. oktober 2011 fremgår, at SST ikke umiddelbart kunne redegøre for, hvorfor forbindelse 6 på tegningen var beskrevet som en "fast fiberforbindelse (mPLS)", men at SST mente, at Datatilsynet selv havde udtalt (i en gammel sag), at MPLS er det samme som fast fiberforbindelse. SST vidste ikke umiddelbart, om der var andre leverandører end TDC involveret i forbindelse 6.

SST har i skemaet, der blev udfyldt som forberedelse til mødet d. 30. maj 2011, oplyst, at data sendes ukrypteret via DSDN (Sundhedsdatanettet) efter beslutning om, at DSDN er et lukket netværk. Det er ikke nærmere angivet, hvad der er grundlaget for beslutningen om, at Sundhedsdatanettet er et lukket netværk.

---

[9] http://www.medcom.dk/wm110009

Ad. 3. - Datatilsynets vurdering
Datatilsynet skal bemærke, at tilsynets udtalelse (j.nr. 2002-711-0028) dateret 21. juni 2002 ikke sidestiller MPLS-separering af data med sikkerheden i faste forbindelser.

Datatilsynet skal endvidere bemærke, at udtalelsen fra 2002 ikke angiver, at MPLS er det samme som fast fiberforbindelse. Udtrykkene "fast forbindelse" og "fast fiberforbindelse" indgår ikke i udtalelsen.

Den omhandlende udtalelse (j.nr. 2002-711-0028) er baseret på en specifik beskrivelse af et konkret netværk, givet til tilsynet af Tele Danmark i 2002. Det er ikke en generel udtalelse, der kan lægges til grund for alle typer af MPLS-netværk. Udtalelsen er langt mere detaljeret end den fremstilling, som er angivet i MedComs notat og på MedComs hjemmeside.

Datatilsynet mener således, at SST ikke uden videre kan basere sine vurderinger på dette grundlag. Den sikkerhedsmæssige vurdering bør baseres på en aktuel undersøgelse af de konkrete netværk, der aktuelt anvendes til datatransmission, hvor SST er dataansvarlig

Angående SST's oplysning om, at data sendes ukrypteret via Sundhedsdatanettet efter beslutning om, at Sundhedsdatanettet er et lukket netværk, bemærker Datatilsynet, at der findes meget forskellige betydninger af udtrykket "lukket netværk". En klassificering af et netværk som "lukket" er i sig selv ikke ensbetydende med, at datatransmissioner gennem netværket er beskyttet tilstrækkeligt set i forhold til databeskyttelsesreglerne.

For at kunne vurdere, hvilke foranstaltninger (kryptering eller andre foranstaltninger) der er nødvendige for at beskytte en datatransmission, er det nødvendigt at kende de faktiske forhold, og tilsynet vil anbefale, at SST undersøger Sundhedsdatanettets faktiske opbygning, og ud fra dette vurderer behovet for sikkerhedsforanstaltninger.

4. Transmissionsveje gennem Sundhedsdatanettet
Af SST's tegning fra mødet den 25. oktober 2011 (bilag 2) fremgår, at kun to regioner er tilsluttet Sundhedsdatanettets knudepunkt (SDX) via MPLS-netværk, altså forbindelsestype 6. De andre regioner er ikke tilsluttet via MPLS-netværk men via et VPN gennem internettet, altså forbindelsestype 5. Af Datatilsynet brev af 2. november 2011 fremgår, at SST under mødet oplyste, at alle regioner med tiden vil gå over til at anvende MPLS.

Af et notat fra MedCom[10] fremsendt som en del af SST's redegørelse den 22. november 2011 fremgår, at alle regioner er tilsluttet via SDN MPLS.

[10] "Aftalesystemet - Notat om Sundhedsdatanettets sikkerhedsmodel". Skrevet af Medcom og dateret den 10. november 2011.

Region H har ved inspektion den 8. december 2011 oplyst til Datatilsynet, at opkobling til Sundhedsdatanets knudepunkt (SDX) sker med minimum to forskellige MPLS-netværk, men ingen af disse netværk er SDN MPLS. SST er dataansvarlig for en datatransmission, der anvender det ene af disse MPLS-netværk (LPR-data sendt fra SST til regionerne - se bilag 1).

Ad. 4. - Datatilsynets vurdering
Det er uklart for Datatilsynet, hvordan forholdene på dette punkt reelt er.

Ved sammenligning af SST's tegning (bilag 2) med notatet fra MedCom fremsendt som en del af SST's redegørelse af 22. november 2011, finder Datatilsynet, at der er uoverensstemmelse i oplysningerne fra SST angående, hvilke regioner der er koblet til Sundhedsdatanettets knudepunkt (SDX) via forbindelse 5, og hvilke der er koblet via forbindelse 6. SST har via tegningen oplyst, at kun to regioner anvender MPLS, mens SST via redegørelsen har oplyst, at alle regioner anvender SDN MPLS.

Ved sammenligning af oplysninger fremkommet ved inspektion hos Region H med notatet fra MedCom fremsendt som en del af SST's redegørelse af 22. november 2011 er der uoverensstemmelse i oplysningerne fra SST og fra Region H angående, hvilke MPLS-netværk der anvendes til datatransmission mellem Region H og Sundhedsdatanettets knudepunkt (SDX). SST har oplyst, at der anvendes SDN MPLS, mens Region H har oplyst, at der ikke anvendes SDN MPLS til den datatransmission, hvor SST er dataansvarlig.

SST er dataansvarlig for nogle af de datatransmissioner, der sker gennem forbindelse 5 og 6, hvor der er disse uoverensstemmende beskrivelser af, hvad forbindelserne består af.

Datatilsynet finder, at SST skal afklare, hvorledes datatransmissionen foregår, der hvor SST er dataansvarlig og sikre sig, at transmissionen foregår sikkerhedsmæssigt forsvarligt.

5. Kontrol med sikkerhedsforanstaltninger ved datatransmission via Sundhedsdatanettet
Som det fremgår af Datatilsynets brev af 2. november 2011, har SST oplyst, at sikkerheden i DSDN-knudepunktet (Sundhedsdatanettets knudepunkt, også benævnt SDX) var blevet undersøgt efter mødet d. 30. maj 2011 ved, at SST spurgte MedCom, hvorledes persondataloven og sikkerhedsbekendtgørelsen sikres efterlevet i knudepunktet. MedCom havde som svar returneret to auditrapporter fra Veritas angående efterlevelse af DS484 og ISO27001. SST kunne ikke ud fra disse rapporter redegøre for efterlevelsen af persondatalovens § 41, stk. 3-5.

Det fremgår af samme brev, at SST ikke har forsøgt at påse efterlevelse af persondatalovens § 41, stk. 3-5, hos de leverandører, som er angivet i bilag 2 (Axcess, TDC, NetDesign, Netic, Logica, TDC Hosting). Disse leverandører er ifølge tegningen i bilag 2 alle involveret i datatransmissioner, hvor SST er dataansvarlig.

Ad. 5. - Datatilsynets vurdering
I forlængelse af det under punkt 4 anførte, skal Datatilsynet gøre opmærksom på, at persondatalovens § 42, stk. 1 angiver, at når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker.

Datatilsynet finder, at SST fremadrettet bør være opmærksom på de forpligtelser, som efter persondataloven påhviler den dataansvarlige i forhold til databehandlere. Når SST skal påse, at datasikkerhed iagttages hos en databehandler, kan dette eksempelvis ske ved at indhente en årlig revisionserklæring fra en uafhængig tredjepart, såfremt revisionen dækker relevante dele af persondataloven.

Tilsynet har noteret sig, at NSI har aftalt med MedCom, at der fastlægges en procedure for indhentning af revisionserklæringer baseret på persondataloven og sikkerhedsbekendtgørelsen jf. SST's brev af 22. november 2011. Tilsynet skal hertil bemærke, at SST skal sikre sig, at denne procedure omfatter alle dele af datatransmissionerne, hvor SST er dataansvarlig, herunder Sundhedsdatanettets knudepunkt, diverse MPLS-netværk og dele, som eventuelt ikke er omfattet af samarbejdet med MedCom.

6. Forsendelse af forskningsdata
Under mødet d. 30. maj 2011 oplyste SST, at data i form af følsomme persondata til f.eks. forskere kan blive lagt ukrypteret på en CD-ROM, som sendes med anbefalet post. SST har efterfølgende oplyst, at SST på en tidligere datatilsynsinspektion har fået indtryk af, at almindelig post er tilstrækkelig.

Datatilsynet er bekendt med, at USB-pinde med persondata er bortkommet i forbindelse med almindelig postforsendelse. Henset til at der er tale om følsomme personoplysninger og, at der kan være tale om store datamængder omfattende mange borgere, vil tilsynet generelt anbefale, at sådanne data krypteres under forsendelse af lagringsmedier.

Datatilsynet skal samtidig henlede opmærksomheden på, at ifølge Digitaliseringsstyrelsen vil det i løbet af 2013 og 2014 blive obligatorisk for borgere og virksomheder i Danmark at have en Digital Postkasse, hvormed der kan kommunikeres sikkert med offentlige myndigheder via log-in med NemID. Alle offentlige myndigheder, virksomheder og borgere i Danmark har endvidere i flere år haft mulighed for at kommunikere sikkert via e-mail.

Opsummering
Datatilsynet anbefaler, at SST gør følgende:

- Undersøger Sundhedsdatanettets faktiske opbygning og afklarer, hvorledes datatransmissionen foregår, og ud fra dette vurderer de faktiske sikkerhedsmæssige forhold i alle datatransmissioner, hvor SST er dataansvarlig, og såfremt undersøgelsen tilsiger dette, iværksætter fornødne sikkerhedsmæssige tiltag.

- Sikrer sig, at der er indgået databehandleraftaler, som lever op til persondataloven og sikkerhedsbekendtgørelsen, herunder præciserer overfor sine databehandlere, at disse er underlagt persondatalovens krav.
- Er opmærksom på sin tilsynsforpligtelse efter persondataloven i forhold til databehandlere.
- Sørger for, at anmeldelser til Datatilsynet angiver alle databehandlere.

Datatilsynet vil i øvrigt foreslå, at SST overvejer brug af end-to-end kryptering[11] med tilstrækkelig styrke[12]. Hvis hele datatransmissionen er beskyttet på denne måde, og ingen parter undervejs har mulighed for at dekryptere data, vil fordelen normalt være, at man nemmere og bedre kan sikre fortrolighed og integritet. End-to-end kryptering er navnlig relevant at overveje, hvis ikke alle dele af en datatransmission er belyst.

Datatilsynet anser hermed denne inspektion for afsluttet. De omhandlende problemstillinger kan blive taget op ved senere lejlighed.

Med venlig hilsen

Walther Starup-Jensen og Henrik Blumensaath Bjarnholt

Bilag 1: Datatilsynets opsummerede beskrivelse af de 4 typer af dataoverførsler, som der fokuseres på.
Bilag 2: SST's tegning af Sundhedsdatanettet med forklaring og angivelse af dataansvar. Denne tegning blev lavet af SST på mødet d. 25. oktober 2011.
Bilag 3: Anmeldelse af databehandling og ændringsanmodninger for "Landspatientregisteret", Datatilsynets journalnummer 2007-54-0206.

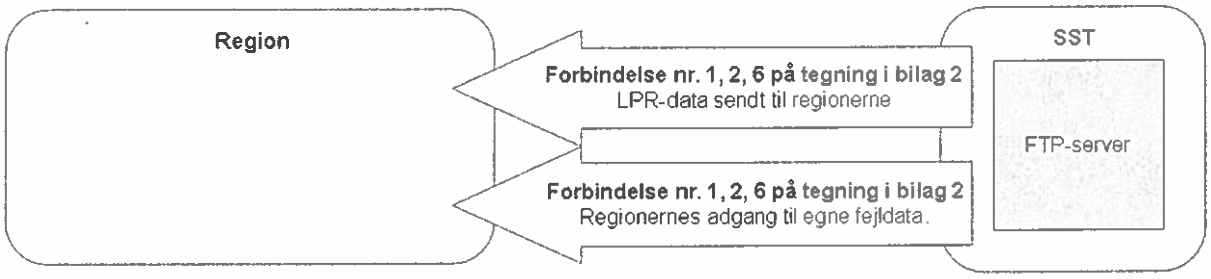
[11] *End-to-end* kryptering betyder: (i) at indholdsdata krypteres hos afsenderen inden afsendelsen, (ii) at indholdsdata er og forbliver krypteret under hele transmissionen (infrastrukturen), og (iii) at indholdsdata først dekrypteres hos den rette modtager efter modtagelsen.
[12] Før at en kryptering har tilstrækkelig styrke, skal krypteringsnøglerne være af en passende længde/kompleksitet og der skal benyttes en anerkendt standard. Hvad der er passende, afhænger af tidspunktet for kryptering samt, hvor lang tid det er nødvendigt, at krypteringen skal kunne beskytte oplysningerne.

Bilag 1

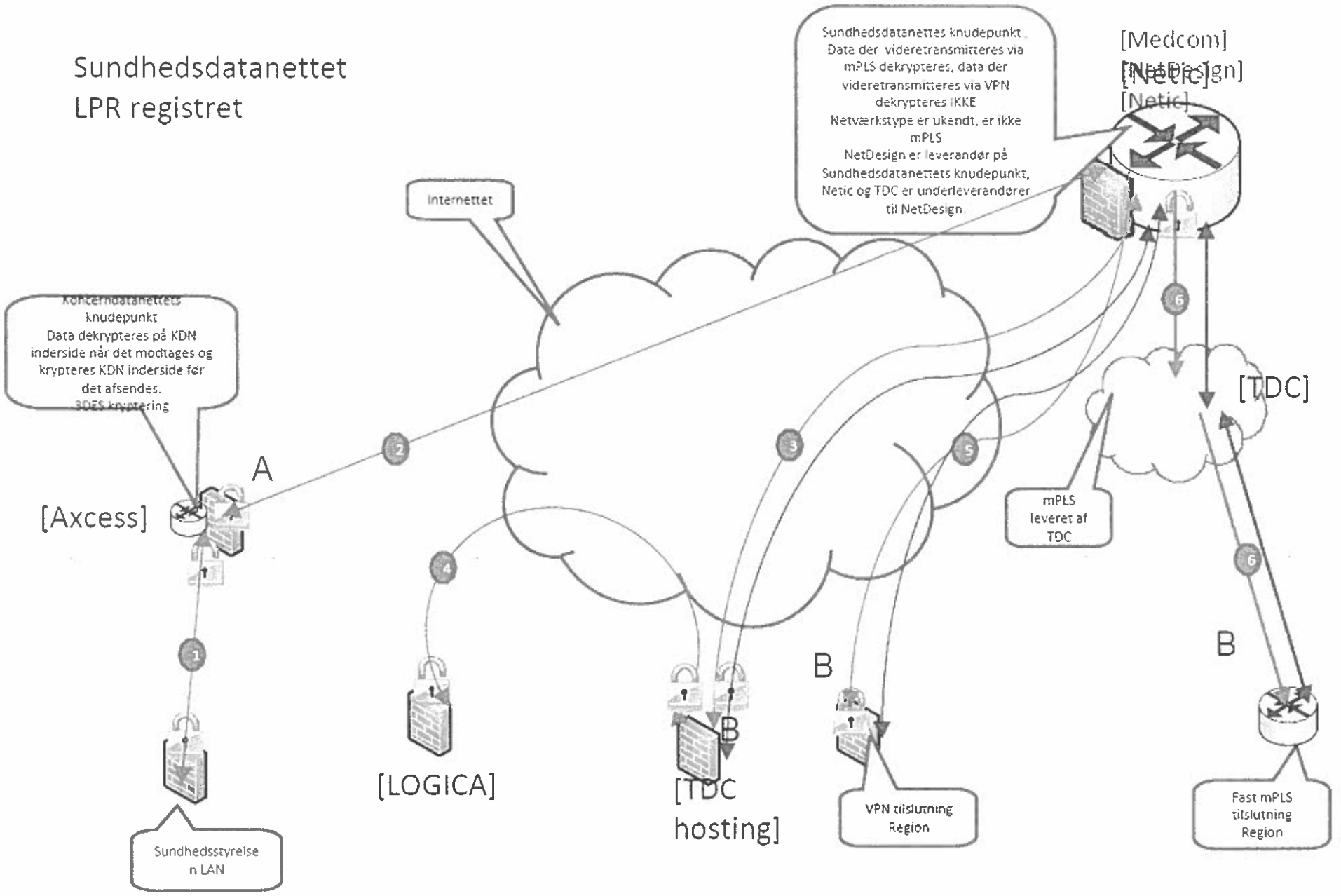
Datatilsynets opsummerede beskrivelse af de to typer af dataoverførsler, som der fokuseres på.

De to transmissioner er her beskrevet på den måde, som Datatilsynet har opfattet dem under mødet den 30. maj 2011, hvor SST udleverede en tegning over diverse datatransmissioner. Betegnelsen på pilene er taget fra SST's beskrivelse. Tilsynet har dog tilføjet en reference til forbindelsesnumrene på tegningen i bilag 2.

I figuren er Region Hovedstaden brugt som eksempel, idet kommunikationen til andre regioner kan foregå via andre forbindelser.



Sundhedsdatanettet
LPR registret



31-10-2011 09:01

Forklaring til tegningen: Sundhedsdatanettet- LPR registret.

Blå forbindelser angiver at Sundhedsstyrelsen har dataansvar frem til firewall hos datamodtager, rod forbindelse angiver at regionerne har dataansvar frem til firewall når de fremsender data/eller fra firewall når de henter data (fejlregister).

1) Sort fiberforbindelse mellem SSTs Lan og Indenrigs- og Sundhedsministeriets Koncerndatanet.
Koncerndatanettet er opbygget af dedikerede fibre der lejes af Forsvarets Informatik og en mPL . Forsvarets Informatik har ingen adgang til de data der transmitteres på de lejede fibre. MPLS skyens del af koncerndatanettet anvendes ikke til transmission af LPR data.

2)Indenrigs- og Sundhedsministeriets VPN forbindelse til Sundhedsdatanettet, trafikken krypteres, ved trafik til parter der anvender VPN forbindelse til Sundhedsdatanettet dekrypteres først i modpartens kantudstyr.

3)TDC Hostings VPN forbindelse til Sundhedsdatanettet

4)*Logicas* private VPN forbindelse mellem Logica og TDC Hosting, via denne VPN varetager Logica drift og overvågning af LPR registret. Der udveksles LPR data via denne forbindelse.

5) VPN forbindelse mellem Sundhedsdatanettets knudepunkt og leverandør eller region.

6) Brugere der er tilsluttet Sundhedsdatanettet gennem fast fiberforbindelse (mPLS), gælder region Midt, region Hovedstaden.
Ved parter der er tilsluttet Sundhedsdatanettet gennem en fast fiberforbindelse (mPLS) sker dekryptering af trafikken i det centrale knudepunkt.
Symbolet router henleder til at trafikken routes til flere parter end angivet på tegningen, gælder alle routere.
Firewall symbolet hos Logica, TDC hosting og regioner symboliserer at trafikken fra vores side termineres der, databehandling indefor firewall regules efter indgåede aftaler.
Ud fra MEDCOMs hjemmeside foregår trafikken i VPN forbindelsen gennem en IP sec krypteret tunnel, gælder forbindelse 2, 3 og 5.
Mht. 2, 3 og 5 gælder at NetDesign vil kunne bryde ind og dekryptere trafikken der passerer gennem Sundhedsdatanettes knudepunkt. Øvrige leverandører hvorigennem trafikken passerer, for eksempel CSC, har ingen mulighed for at bryde ind og dekryptere data.

Mht. terminering af 5 og 6. Regionerne kan have flere leverandorer af netværk og systemer. SST kender ikke de fysiske leveringsteder for data. SST afleverer data til afleveringssted angivet med Regionens aftale med Medcom (de blå streger). SST afleverer data til placering, servernavn og formål, angivet af Regionen i henhold til aftale med Regionen . Regionerne kender ikke de fysiske leverings- og afhentningssteder for data. Regionerne henter og afleverer data til afleveringssted angivet med SSTs aftale med Medcom (de røde streger).

Mht. 4, VPN tunnel mellem Logica og TDC Hosting er krypteringsmetode ikke kendt af SST. Fremgår ikke umiddelbart af SSTs kontrakt med Logica. Logica og TDC hosting har adgang til data de behandler.

Mht. 6 gælder at VPN tunnel afsluttes i Sundhedsdatanettes knudepunkt og data transmitteres ukrypteret gennem mPLS til Regionen. SST er ikke bekendt med den aftale Medcom har med TDC fsa.. mPLS, blot at trafikken routes gennem TDC mPLS netværk.

Bilag 3

Journalnummer: 2007-54-0206

Blankettype: Offentlig forvaltning

Anmeldelse af behandlinger der foretages for den offentlige forvaltning.

Bemærk! Hvor andet ikke udtrykkeligt er angivet, vil de oplysninger, der fremgår af anmeldelsesblanketten, blive offentliggjort i Datatilsynets fortegnelse over anmeldte behandlinger. Fortegnelsen er offentligt tilgængelig på Datatilsynets hjemmeside. Felter markeret med * **skal** udfyldes.

1.Dataansvarlig myndighed	Navn Sundhedsstyrelsen Adresse Islands Brygge 67 2300 København S Kommunekode (For kommuner og amter: Angiv kommune- eller amtskode. For øvrige myndigheder: Angiv ressortministerium) Sundheds- og Forebyggelsesministeriet Postnr. 2300 By København S Evt.J.nr./ID.nr. 6-5011-1/1 [X] Oplysningerne opbevares hos den dataansvarlige og/eller [X] Oplysningerne opbevares hos databehandler Databehandlerens navn National Sundheds-IT, Logica Danmark A/S og Den fælles offentlige sundhedsportal, Sundhed.dk Databehandlerens adresse Henholdsvis Islands Brygge 39, 2300 København S, Lautrupvang, 2750 Ballerup og Dampfærgevej 22, 2100 København Ø

2. Betegnelse og formål	Behandlingens betegnelse: Landspatientregisteret Behandlingens formål og evt.delformål: a)Danne grundlag for Sundhedsstyrelsens løbende sygehusstatistik. b)Danne grundlag for sundhedsøkonomiske beregninger i institutioner under Sundheds- og Forebyggelsesministerets ressortområde (takstberegning), c)Forsyne de myndigheder, der er ansvarlige for sygehusplanlægningen med det nødvendige beslutningsgrundlag d)Forsyne de myndigheder, der er ansvarlig for tilsyn med det nødvendige datagrundlag. e)Indgå som grundmateriale i forbindelse med overvågning af hyppigheden af forskellige sygdomme og behandlinger. f)Bidrage til den medicinske forskning. g)Bidrage til kvalitetssikring i sygehusvæsenet h)Give sundhedsfagligt uddannet personale adgang til medicinske og administrative data vedrørende tidligere sygehusbehandling på afdelinger for patienter, der er taget i behandling. Behandlingen skal udelukkende finde sted i videnskabelig eller statistisk øjemed [ ] Ja [X] Nej Behandlingen skal udelukkende finde sted med henblik på at føre et retsinformationssystem [ ] Ja [X] Nej

3. Generel beskrivelse	Følgende typer af behandling indgår: Indsamling af patientoplysninger fra offentlige sygehuse, private sygehuse/klinikker samt kommunale sundhedscentre/klinikker. Oplysningerne tilvejebringes ved direkte overførsel eller på maskinlæsbare medier fra de enkelte sygehuskommuners hospitalsinformationssystemer eller for Det Fælleskommunale hospitalsinformationssystem, fra private sygehuse klinikker samt kommunale sundhedscentre/klinikker. Oplysninger vedrørende fødende kvinder uden for sygehus og børn født uden for sygehus (hjemmefødsler) indhentes på skemaer og overføres til maskinlæsbart medie. Der foretages kontrol til sikring af, at der ikke registreres urigtige eller vildledende oplysninger i form af fejlsøgning. Oplysninger, der viser sig urigtige eller vildledende, bliver snarest muligt slettet eller berigtiget. Databehandling består i fejlsøgning, ajourføring samt produktion af uddata til statistik, tilsyns- eller planlægningsmæssig anvendelse, til ajourføring af andre registre i Sundhedsstyrelsen (bl.a. Cancerregisteret) samt uddata til de under punkt 5 nævnte modtagere. Der foretages samkøring med Sundhedsstyrelsens øvrige registre med henblik på produktion af uddata til statistik, tilsyns- eller planlægningsmæssig anvendelse. Der vil blive foretaget samkøring/sammenstilling af oplysninger i kontroløjemed [X] Nej [ ] Ja, med hjemmel i følgende lov: Der indgår manuelle registre i behandlingen [ ] Ja [X] Nej Der påtænkes truffet afgørelser udelukkende på grundlag af elektronisk databehandling [ ] Ja [X] Nej Der behandles følgende følsomme oplysninger: [ ] Racemæssig eller etnisk baggrund [ ] Politisk overbevisning [ ] Religiøs overbevisning [ ] Filosofisk overbevisning [ ] Fagforeningsmæssige tilhørsforhold [X] Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v. [ ] Seksuelle forhold Der behandles følgende andre oplysninger om enkeltpersoners

	rent private forhold? [ ] Strafbare forhold [ ] Foreningsmæssige forhold [ ] Væsentlige sociale problemer [ ] Andet
4.Kategorier af registrerede og oplys-ningstyper	Der behandles oplysninger om følgende kategorier af personer: A) Personer der siden 1. januar 1977 har været i stationær, ambulant eller skadestuebehandling eller har været til undersøgelse, genoptræning på et offentligt eller privat sygehus/klinik. Personer der føder udenfor sygehus og børn født uden for sygehus (hjemmefødsler). B) C) D) E) F) Der behandles følgende typer af oplysninger om de ovenfor angivne kategorier af personer: ad A) Personoplysninger (cpr-numre, bopælskommune), indlæggelses- og udskrivningsoplysninger, tidsangivelser for hændelser under sygdomsforløb, diagnoseoplysninger, oplysninger om undersøgelser og behandlinger, genoptræning herunder operationer, årsag til ventetid, supplerende oplysninger vedrørende fødsler, herunder fødsler udenfor sygehus. ad B)

	ad C) ad D) ad E) ad F)
5. Modtagere	Oplysningerne kan overføres til følgende modtagere eller kategorier af modtagere: Alle eller dele af oplysninger kan overføres til modtagere eller kategorier af modtagere. Private eller offentlige forskere. Institutioner under Sundheds- og Forebyggelsesministeriets ressortområde. Kvalitetsdatabaser, Danmarks Statistik, Det Psykiatriske Centralregister. Statens Institut for Folkesundhed. Sygehuse, regioner og kommuner til anvendelse af oplysninger i behandlings- eller planlægningsøjemed, Sundhedsfagligt uddannet personale til anvendelse i behandlingsøjemed. Oplysninger vedrørende patienter bosiddende i en region, der har været i behandling på andre end egne sygehuse, kan videregives til den pågældende region til brug for den lokale sygehusplanlægning og forskning. Arbejdsskadestyrelsen (Arbejdsskadestyrelsens Kræftregister). Sundhedsstyrelsens direktør kan autorisere brugere til at have terminaladgang til en krypteret udgave af Landspatientregisteret (ingen personnumre).
6. Tredjelande	Der påtænkes overført oplysninger til tredjelande: [X] Nej [ ] Ja, overførslen sker med følgende formål:
7. Sikkerhed	Der træffes sikkerhedsforanstaltninger, som beskrevet i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 kapitel 1 og 2 [X] Ja [ ] Nej Der træffes sikkerhedsforanstaltninger som beskrevet i Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 kapitel 3

	[X] [ ]	Ja Nej Evt. yderligere sikkerhedsforanstaltninger:
8. Påbegynd-else	Tidspunkt for påbegyndelse af behandling:	Dato Behandling påbegyndtes inden lovens ikrafttræden.
9.Sletning	Tidspunkt for sletning af oplysninger: Alle oplysninger i registeret, der kan henføres til bestemte personer, slettes 50 år efter optagelser i registeret.	
Note fra Datatilsynet		