SUNDHEDSDATA-
STYRELSEN

Vejledning om informations-sikkerhed i sundhedsvæsenet

April 2016

Vejledning om informationssikkerhed i sundhedsvæsenet

Version: 1.0
Dato: 19/4 - 2016

Sundhedsdatastyrelsen
Ørestads Boulevard 5

2300 København S

www.sundhedsdatastyrelsen.dk

© Sundhedsdatastyrelsen
Rapporten kan frit refereres med tydelig kildeangivelse.

Indholdsfortegnelse

0. Ledelsesresumé 6

1. Baggrund, formål og målgruppe 8

1.2 Afgrænsninger 9

1.3 Arbejdsgruppens sammensætning 10

2. Læsevejledning 11

3. Adgang til oplysninger – lovkrav 13

3.1 Behandlingsøjemed 16

3.1.1 Journalføringspligt og sundhedspersoners adgang til patientoplysninger 16

3.1.2. Videregivelse af oplysninger til behandlingsformål 17

3.1.3 Elektronisk indhentning af patientoplysninger 18

3.1.4 Samtykke og retten til at frabede sig indhentning eller videregivelse til behandlingsformål 20

3.1.5 Værdispringsreglen 22

3.1.6 Beslutningsgraf vedr. sundhedspersoners elektroniske indhentning af patientoplysninger 22

3.2 Sekundær anvendelse af helbredsoplysninger 23

3.2.1 Administration, herunder ledelsesinformation og afregning 24

3.2.2 Kliniske kvalitetsdatabaser 26

3.2.3 Videnskabelige og statistiske undersøgelser 26

3.2.4 Videregivelse og oplysninger til tilsynsmyndigheder og til behandlingen af klage- og erstatningssager 28

3.2.5 Videregivelse til politiet 29

3.2.6 Andet 30

3.2.7 Tilbagekaldelse af samtykke 30

3.2.8. Videregivelse til andre – offentlighedsloven 30

4. Dataansvar 31

4.1 Den dataansvarliges forpligtelser 32

4.2 Hjemmel til behandling af oplysninger 33

4.3 Databehandlere 35

4.3.1 Indholdet af den skriftlige databehandleraftale 36

4.4 Anmeldelse til Datatilsynet 37

4.4.1 Den offentlige sektor 37

4.4.2 Den private sektor 40

4.4.4 Anmeldelse på Datatilsynets hjemmeside 41

4.5 Overblik over dataflow 41

5. Deling af oplysninger på tværs af sektorer 44

5.1 Hvordan deles oplysninger? 45

5.2 Betingelser for deling af oplysninger på sundhedsområdet 45
5.3 Landsdækkende databaser 48
6. Adgang til borgerens oplysninger 49
7. Borgerens adgang til oplysninger 51
7.1 Ret til indsigt og aktindsigt 51
7.2 Adgang til egne sundhedsoplysninger 52
7.3 Adgang til logoplysninger 53
7.4 Adgang for pårørende, værger m.v. 54
7.4.1 Forældremyndighed eller værgemål 54
7.4.2 Samtykke og fuldmagt 54
7.4.3 Dødsfald 55
8. Anvendelse af personoplysninger til videnskabeligt eller statistisk formål 57
8.1 Sundhedsvidenskabelig forskning på mennesker eller biologisk materiale 57
8.2 Videnskabelige og statistiske undersøgelser på basis af patientjournaler 59
8.3 Registerforskning 59
8.5 Biobanker 60
8.5 Opbevaring og logning 61
8.6 Videregivelse til andre forskningsprojekter 62
8.7 Offentlig eller privat forskning 63
8.8 Pseudonymisering og anonymisering 63
8.8.1. Pseudonymisering 63
8.8.2 Anonymisering 63
8.9 Big data 64
9. Overførsel af patientoplysninger til EU- og tredjelande 65
9.1 Krigsregelen 66
9.2. Særligt vedr. videnskabelige og statistiske undersøgelser 67
9.2 Beskyttelse af personoplysninger ved rejse i udlandet 67
10. Netværkssikkerhed 68
10.1 Intern kommunikation 68
10.2 Ekstern kommunikation 69
10.2.1 Internettet 69
10.2.2 Sundhedsdatanettet 70
10.3 Den nationale serviceplatform 71
11. Mobil sikkerhed 73
11.1 Hvad er mobile enheder? 73
11.2 Trusler 74

11.3 Løsninger 74
12. Krav vedr. informationssikkerhed 77
12.1 Informationssikkerhed er mere end it-sikkerhed 77
12.2 Anvendelse af standard for informationssikkerhed 77
12.2.1. Ledelsesværktøj 78
12.2.2. Risikovurdering 79
12.3 Cybersikkerhed 79
12.3.1 Medarbejdere og adfærd 79
12.4 Sikker udvikling af it-løsninger 80
12.41. Apps som medicinsk udstyr 80
12.4.2 Test 81
Bilag 1 Litteraturliste 82

0. Ledelsesresumé

Denne vejledning er udarbejdet med henblik på at skabe et fælles grundlag for arbejdet med informationssikkerhed i sundhedsvæsenet. Målgruppen for vejledningen er de ansvarlige for informationssikkerheden, der skal sikre, at der tages de beslutninger, der er nødvendige for at beskytte borgernes oplysninger.

Lovgrundlaget for anvendelsen af personoplysninger i sundhedsvæsenet findes i mange forskellige love, og vejledningen beskriver med udgangspunkt i konkrete anvendelsessituationer: behandling af patienten, videnskabelige undersøgelser eller administrative opgaver, hvilke lovregler, der regulerer f.eks. indsamling, videregivelse og elektronisk indhentning.

I den forbindelse beskriver vejledningen også regelgrundlaget fra persondataloven vedr. den dataansvarliges ansvar og opgaver. Der har i de seneste år været en række sager, hvor det har vist sig, at lovgrundlaget for databehandlingen ikke har været overholdt, f.eks. i forbindelse med Dansk Almen Medicinsk Database (DAMD), hvor der foregik dataindsamling, der ikke var hjemmel til i lovgivningen. Og vejledningen bidrager her med anbefalinger til, hvordan man som dataansvarlig inden databehandlingen igangsættes, kan sikre sig, at der er lovhjemmel og at man har indgået de nødvendige aftaler om databehandlingen.

> Hjemmel er et grundlæggende juridisk princip, hvorefter offentlige myndigheders konkrete afgørelse og generelle administrative forskrifter skal have støtte (hjemmel) i lovgivningen.

Borgernes inddragelse i deres egen behandling er et politisk mål, som ønskes understøttet gennem, at de både bidrager med informationer digitalt og at de har indsigt i, hvad der er registreret om dem og deres behandling. I vejledningen er grundlaget for borgernes og deres pårørendes adgang til oplysningerne beskrevet med henblik på, at man i sundhedsvæsenet kan understøtte borgernes rettigheder på den bedste måde.

Helbredsoplysninger anvendes i vidt omfang til videnskabelige og statistiske undersøgelser, der skal bidrage til at finde sygdomsårsager, udvikle nye behandlingsformer o.l. Danmark har en unik position ved, at borgerne har en meget stor tillid til, at deres oplysninger behandles fortroligt og til formål, der er vigtige for samfundet. Det er vigtigt, at denne tillid bevares, og derfor beskriver vejledningen både de gældende retningslinjer for videnskabelige og statistiske undersøgelser og kommer med en række anbefalinger til, hvordan man kan sikre sig, at oplysningerne ikke kommer i de forkerte hænder.

Der er krav om, at standarden for informationssikkerhed ISO/IEC 27001 implementeres i alle statslige institutioner og den opfattes som best practice i forhold til regioner og kommuner. Digitaliseringsstyrelsen har udgivet en række vejledninger om implementering af ISO27001 og i denne vejledning er der derfor kun medtaget anbefalinger på nogle områder, som anses for at være ekstra relevante i forhold til følsomheden af de oplysninger, der behandles i sundhedsvæsenet.

Vejledningen vil være et dynamisk dokument, som løbende vil blive opdateret i forhold til ny lovgivning, nye tekniske muligheder og andre forhold vedr. digitalisering af sundhedsvæsenet, som giver sikkerhedsmæssige udfordringer.

1. Baggrund, formål og målgruppe

Sundhedsstyrelsen udgav i 2008 "Informationssikkerhed - vejledning for sundhedsvæsenet". Baggrunden for vejledningen var de netop gennemførte ændringer i sundhedsloven vedr. sundhedspersoners adgang til elektroniske systemer i forbindelse med behandling af patienter.

Det er nu 8 år siden, Sundhedsstyrelsens vejledning blev udgivet og siden da er der sket ændringer i lovgivningen på området, men lige så vigtigt er det, at it-anvendelsen i sundhedsvæsenet er blevet mere omfattende og at der er etableret et tættere samarbejde mellem de forskellige parter i sundhedsvæsenet.

Sundhedsdatastyrelsen (tidligere National Sundheds-it) nedsatte i maj 2015 en arbejdsgruppe med det formål at revidere den eksisterende vejledning og i nødvendigt omfang belyse relevante problemstillinger i relation til informationssikkerhed, som den stigende digitalisering i sundhedsvæsenet har skabt.

Formålet med den foreliggende vejledning er dels at beskrive, hvordan lovgrundlaget for behandling af patientoplysninger skal og kan håndteres hos sundhedsvæsenets parter, dels at komme med anbefalinger til, hvordan man etablerer et tilstrækkeligt informationssikkerhedsniveau i sundhedsvæsenet. Øget samarbejde mellem parterne i sundhedsvæsenet gør det nødvendigt, at man har en fælles forståelse og et fælles grundlag for, hvordan lovgivningen skal fortolkes og hvordan lovkrav og best practice kan implementeres, så det på samme tid understøtter en sikker håndtering af borgernes følsomme oplysninger og fremmer digitaliseringen som understøttende for en sammenhængende patientbehandling.

Vi er opmærksomme på, at sikkerhedsniveauet altid skal fastlægges i en afvejning mellem hensynet til informationssikkerhed og hensynet til organisationens eller virksomhedens forretningsmål, økonomi m.v. Dog er det en grundlæggende præmis for vejledningen, at lovgivningen skal overholdes.

Vejledningen er ikke udtømmende i forhold til, hvordan man sikrer det informationssikkerhedsniveau, der er nødvendigt for at sikre en tilstrækkelig beskyttelse af behandlingen af personoplysninger.

Dels har vi valgt at henvise til andre – mere generelle - vejledninger, som er relevante også for sundhedsvæsenet, herunder ISO/IEC 27001 og 27002 Standard for informationssikkerhed, som nærmere beskriver relevante organisatoriske og tekniske sikringsforanstaltninger. Dels er det tanken, at der i relation til vejledningen skal udarbejdes mere specifikke anbefalinger, skabeloner o.l. rettet mod de forskellige målgrupper.

Den primære målgruppe for vejledningen er alle, der har ansvar for data- og informationssikkerhed i sundhedsvæsenet, både hos mindre, private aktører som praktiserende læger og hos ledelsen i regioner og kommuner. Ligeledes er vejledningen

relevant for de ledere, der skal sikre, at medarbejderne i dagligdagen kender og efterlever de regler, der gælder for behandlingen af fortrolige og følsomme personoplysninger.

Herudover er der dele af vejledningen, som vil være relevante for it-funktioner i regioner og kommuner, informationssikkerhedsansvarlige og leverandører af it-løsninger til sundhedsvæsenet.

Dele af vejledningen vil være relevant for apotekere og farmakonomer, selvom disse ikke defineres som sundhedspersoner i sundhedsloven.

Vejledningen er ikke primært rettet mod medarbejderne i sundhedsvæsenet, men det er Sundhedsdatastyrelsens hensigt, at der med baggrund i vejledningen udformes behovsbaseret informationsmateriale målrettet specifikke faggrupper eller områder inden for sundhedsvæsenet.

Udviklingen inden for sundheds it-området går så hurtigt i disse år, at det efter arbejdsgruppens opfattelse vil være hensigtsmæssigt at opfatte vejledningen som et dynamisk dokument, der revideres løbende efter behov. Vejledningen vil derfor primært være et elektronisk dokument, og Sundhedsdatastyrelsen er ansvarlig for en årlig revision af dokumentet.

1.2 Afgrænsninger

I forbindelse med udarbejdelse af vejledningen har arbejdsgruppen fravalgt at behandle den kommende EU-persondataforordning, idet den endnu ikke var vedtaget ved afslutningen af arbejdsgruppens arbejde.

Forordningen afløser det eksisterende persondatadirektiv i 2018. Dette vil medføre en række yderligere forpligtelser for dataansvarlige og databehandlere, ligesom det vil afstedkomme ændringer i dansk følgelovgivning.

Da Justitsministeriets udmelding vedr. forordningens betydning for gældende dansk ret endnu ikke foreligger, vil de ændringer, som følger af persondataforordningen, blive indarbejdet i næste version af vejledningen 2016 eller når der foreligger konkrete udmeldinger fra Justitsministeriet.

Der har i sundhedsvæsenet været uklarhed om det retlige grundlag for kvalitetsarbejde, herunder journalaudits. Sundheds- og Ældreministeriet vil på denne baggrund udarbejde forslag til en mere entydig og klar regulering.

Når denne afklaring foreligger, vil det blive indarbejdet i vejledningen i forbindelse med den årlige revision.

Ligeledes har arbejdsgruppen vurderet, at implementering af ISO/IEC 27001 (Standard for informationssikkerhed) ikke medtages.

Vejledningens fokus har primært været at beskrive, under hvilke betingelser man må behandle personoplysninger. Der beskrives ikke konkrete organisatoriske eller tekniske sikringstiltag, men henvises til standarden for informationssikkerhed ISO/IEC 27001 som grundlag herfor.

1.3 Arbejdsgruppens sammensætning

Arbejdsgruppen, som har udarbejdet vejledningen, har bestået af:

Anne Schultz, Region Syddanmark
Bodil Grøn, Fredericia Kommune
Lene Olsen, Kalundborg Kommune
Lars Stig Jørgensen, Region Sjælland
Eddie Nielsen, praktiserende læge, Ålborg
Niels Holm, praktiserende læge, Roskilde
Katrine Stokholm, Danske Regioner
Frederik Enelund, Sundheds- og Ældreministeriet
Jesper Thykier, sundhed.dk
Jens Rahbek Nørgaard, MedCom
Mette Bjørn Andersen, DI ITEK (til 1.10.2015)
Henning Mortensen, DI Digital (fra 1.10.2015)
Marchen Lyngby, Sundhedsdatastyrelsen
Pia Jespersen, Sundhedsdatastyrelsen (formand)

2. Læsevejledning

Vejledningen tager sit udgangspunkt i den lovgivning, som er gældende for sundhedsområdet, og beskriver, hvordan den eller de ansvarlige for informationssikkerheden organisatorisk og teknisk kan sikre sig, regler og best practice efterleves.

Kapitlerne 3 og 4 fokuserer på, hvordan den eksisterende lovgivning skal tolkes.

Kapitel 3 omhandler de regler, der fastlægger, under hvilke betingelser, forskellige faggrupper må få adgang til patientoplysninger. I kapitlet beskrives, hvornår patientoplysninger må videregives eller elektronisk indhentes i forhold til de angivne formål for databehandlingen: Patientbehandling, kvalitetssikring, videnskabelige og statistiske undersøgelser m.v.

I **kapitel 4** beskrives det ansvar, der påhviler den dataansvarlige, herunder krav om anmeldelse til Datatilsynet og indgåelse af databehandleraftaler. Herudover beskriver kapitlet, hvordan man sikrer sig, at der er hjemmel til behandling af personoplysningerne.

I kapitlerne 5-9 beskrives mere konkret, hvordan man på baggrund af lovgivningen kan og skal håndtere dataadgang og informationssikkerhed i forskellige situationer.

Kapitel 5 handler om deling af data mellem de forskellige parter i sundhedsvæsenet. Begrebet "deling" er bevidst valgt som grundlag for kapitlet, da det i den bredere offentlighed er det begreb, der bruges, når man italesætter behovet for at kunne indhente eller videregive oplysninger om patienter med henblik på at skabe et mere sammenhængende sundhedsvæsen med borgeren i centrum.

Kapitel 6 beskriver forhold omkring adgang til borgernes egne data, som de generer til eget brug for at kunne følge deres egen helbredstilstand, mens **kapitel 7** omhandler borgernes og deres pårørendes adgang til deres egne helbredsoplysninger.

Kapitel 8 beskriver, under hvilke omstændigheder patientoplysninger må anvendes til videnskabelige og statistiske formål. Mens kapitel 3 har fokus på, under hvilke omstændigheder, oplysninger fra patientjournaler må videregives til videnskabelige og statistiske formål, uddybes det i dette kapitel, hvordan man i forbindelse med sin undersøgelse skal behandle de indhentede patientoplysninger.

Kapitel 9 omhandler beskyttelse af personoplysninger ved overførsel til andre lande.

Kapitlerne 10-11 omhandler mere tekniske aspekter omkring informationssikkerhed. **Kapitel 10** omhandler netværkssikkerhed og **kapitel 11** mobil sikkerhed.

Endelig bliver der i **kapitel 12** introduceret til anvendelsen af standarden for informationssikkerhed – ISO/IEC 27001, som statslige institutioner er forpligtet til at efterleve og som anses for best practice for regioner og kommuner. Kapitlet beskriver nogle forhold med særlig relevans for sundhedsområdet.

Der er i teksten i stort omfang indsat elektroniske links til de kilder, der har været anvendt. Men internettet er jo en levende organisme, og det kan derfor forekomme, at et link ikke længere virker, fordi man har ændret opsætning e.l. på den hjemmeside, der henvises til. I forbindelse med den årlige revision vil der også blive foretaget en gennemgang af links i vejledningen. Hvis man støder på et link, der ikke længere virker, kan man finde oplysninger om dokumentets navn i litteraturlisten og søge på dette i stedet.

3. Adgang til oplysninger – lovkrav

Adgangen til patientoplysninger er reguleret i flere love.

Det er først og fremmest sundhedsloven, der i relation til patientbehandling og den videre brug af patientjournaler supplerer persondatalovens mere generelle bestemmelser om behandling af personoplysninger.

> Med patientoplysninger menes patientens helbredsforhold, øvrige rent private forhold og andre fortrolige oplysninger, der er relevante for behandlingen af patienten

Sundhedsloven regulerer bl.a. sundhedspersoners videregivelse og indhentning af personoplysninger fra behandlingssammenhænge, dvs. hvem der må få adgang til data, der er registreret i forbindelse med behandling af patienten i f.eks. elektroniske patientjournaler, laboratoriesystemer, lægepraksissystemer o.l.

Det er primært sundhedslovens kapitel 9, der supplerer de generelle regler i persondataloven, men der findes bestemmelser i lovgivningen, som dækker mere specifikke områder.

Persondataloven er den lov, der implementerer EU's databeskyttelsesdirektiv i dansk lovgivning. Dog går regler i anden lovgivning, der giver borgerne en bedre retsstilling, jf. persondataloven[1] forud for reglerne i persondataloven. Eksempelvis går sundhedslovens kapitel 9, der fastlægger betingelserne for adgang til personoplysninger i forbindelse med behandling af patienter, forud for reglerne i persondataloven, idet reglerne er skærpede i forhold til reglerne i af persondataloven.

[1] Persondataloven §2, stk. 1

Persondataloven opererer med 3 typer af personoplysninger. Følsomme oplysninger om menneskers rent private forhold omfatter f.eks. oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold[2].

Andre oplysninger om rent private forhold anses også for at være følsomme, f.eks. oplysninger om strafbare forhold eller væsentlige sociale problemer. De oplysningstyper, der ikke er kategoriseret som følsomme, kaldes almindelige personoplysninger[3].

Almindelige personoplysninger kan f.eks. være identifikationsoplysninger eller oplysninger om økonomiske forhold[4].

Persondataloven opdeler personoplysninger i tre typer: følsomme oplysninger, oplysninger om andre rent private forhold og almindelige personoplysninger. Opdelingen findes, fordi der er forskellige betingelser og procedurer for behandling af oplysninger, afhængig af deres følsomhed.

I forvaltningsloven finder man de generelle bestemmelser om offentligt ansattes tavshedspligt, der gælder ved siden af sundhedslovens regler[5] om tavshedspligt for autoriserede sundhedspersoner.

Autorisationsloven beskriver de forpligtelser, en autoriseret sundhedsperson er underlagt, herunder journalføringspligten, som udmøntet i journalføringsbekendtgørelsen.

I retssikkerhedsloven og serviceloven findes der en række bestemmelser, som på det kommunale område supplerer sundhedslovens og persondatalovens bestemmelser om adgang til personoplysninger for andre end autoriserede sundhedspersoner.

Desuden findes der bestemmelser i lægemiddelloven og apotekerloven, som regulerer adgangen til at indsamle og behandle lægemiddeloplysninger.

I epidemiloven findes bestemmelser om foranstaltninger mod smitsomme og andre overførbare sygdomme, herunder krav om indberetning.

---

[2] Persondatalovens §7

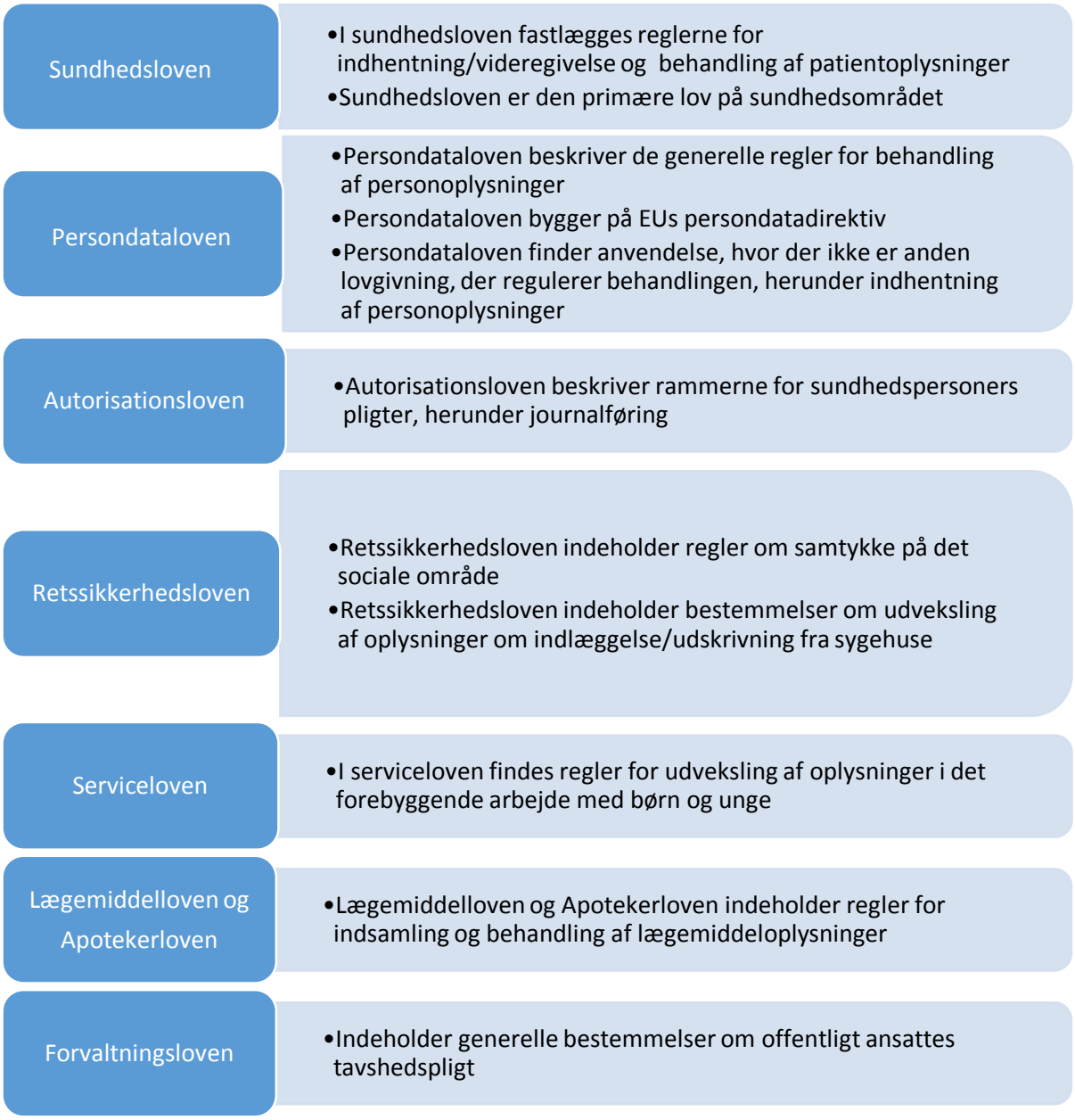
[3] Persondatalovens §8

[4] Persondatalovens §§6 og 11

[5] Sundhedsloven, § 40

Herudover optræder der i anden lovgivning specifikke retningslinjer f.eks. for dataadgang til patientoplysninger. I det omfang, det er relevant, vil de blive berørt i vejledningen.

Nedenstående figur giver en oversigt over, hvad de forskellige love regulerer i forhold til behandling af patientoplysninger.



Figur 1: Primær lovgivning, der fastlægger retningslinjer for behandling af patientoplysninger

I det efterfølgende beskrives reglerne for behandling af personoplysninger, herunder indhentning og videregivelse.

Der er forskellige regler afhængig af, om videregivelsen/indhentningen af oplysninger sker i patientbehandlingsøjemed eller til andre formål.

Reglerne i sundhedsloven gælder alene for sundhedspersoners videregivelse af oplysninger, der stammer fra behandlingssituationer, dvs. oplysninger, der indgår i patientens journal.

Ved sundhedspersoner forstås både personer, der er sundhedsfagligt autoriserede til at varetage sundhedsfaglige opgaver og personer, der arbejder efter delegation fra en sundhedsperson[6].

Hvis andre faggrupper deltager aktivt i forbindelse med patientbehandlingen, kan de få adgang til patientoplysninger, der er relevante for udførelsen af deres opgave. Det kan være elever og studerende, der udfører sundhedsfaglige opgaver i forbindelse med deres uddannelse. Men der kan også være tale om ingeniører, der har ansvaret for medicoteknisk udstyr eller lærere og pædagoger, der indgår i behandlingen på det børnepsykiatriske område[7]. Derfor er det væsentligt, at der foretages en konkret vurdering af den enkeltes funktion og rolle i forbindelse med patientbehandlingen.

Når en ikke-autoriseret sundhedsperson udfører opgaver på vegne af en autoriseret sundhedsperson, må de indhente[8] de samme oplysninger, som den autoriserede sundhedsperson har adgang til, hvis det er nødvendigt for udførelsen af deres opgaver og hvis adgangen teknisk er begrænset til den behandlingsenhed, de er tilknyttet.

3.1 Behandlingsøjemed

I forhold til begrebet behandling og anvendelse af oplysninger i behandlingsøjemed skal man være opmærksom på, at i persondataloven anvendes begrebet *behandling* forskelligt fra det kliniske behandlingsbegreb, idet persondatalovens behandlingsbegreb omhandler al form for behandling af *data*, uanset formålet med databehandlingen.

3.1.1 Journalføringspligt og sundhedspersoners adgang til patientoplysninger

Sundhedspersoner har pligt til at registrere oplysninger, der er relevante for patientens behandling.

I autorisationsloven og den tilhørende journalføringsbekendtgørelse reguleres sundhedspersoners journalføringspligt. Det betyder, at der lovgivningsmæssigt stilles krav om, at autoriserede sundhedspersoner skal føre ordnede optegnelser vedr.

[6] Jf. sundhedslovens §6: Ved sundhedspersoner forstås personer, der er autoriserede i henhold til særlig lovgivning til at varetage sundhedsfaglige opgaver, og personer, der handler på disses ansvar.

[7] Vedr. brug af medhjælp henvises til Bekendtgørelse nr. 1219 af 11. december 2009 om autoriserede sundhedspersoners benyttelse af medhjælp (delegation af sundhedsfaglig virksomhed)

[8] Sundhedslovens §42a, stk. 2

patientens behandling, dvs. at de skal registrere alle oplysninger, der er relevante for behandlingen af patienten.

Journalføringen er med til at skal sikre, at sundhedspersoner har de nødvendige oplysninger til rådighed om patienten i behandlingssituationen.

I forbindelse med sundhedspersoners adgang til patientoplysninger skelner man i sundhedsloven mellem videregivelse og elektronisk indhentning af oplysninger.

3.1.2. Videregivelse af oplysninger til behandlingsformål

Til brug for aktuel behandling af patienten er det muligt for sundhedspersoner at videregive oplysninger til andre sundhedspersoner. Dette skal som udgangspunkt ske med patientens samtykke.

Med videregivelse forstås, at en sundhedsperson giver oplysninger videre til en anden sundhedsperson i forbindelse med den aktuelle behandling af patienten.

Ved videregivelsen skal det vurderes, om materialet indeholder oplysninger, der ikke er nødvendige for den aktuelle behandling. Disse oplysninger må ikke videregives, og den ansvarlige for videregivelsen skal derfor gennemgå materialet for at sikre sig, at det kun indeholder oplysninger, der er relevante for modtagerens behandling af patienten.

> Med videregivelse menes, at en sundhedsperson kan give oplysninger videre til andre sundhedspersoner om patientens helbredsforhold, øvrige rent private oplysninger og andre fortrolige oplysninger.

Videregivelse kan ske elektronisk eller manuelt (papir, fax, telefon).

Det er i visse tilfælde tilladt at videregive oplysninger uden samtykke fra patienten, f.eks. når det er nødvendigt af hensyn til et aktuelt behandlingsforløb for patienten, og videregivelsen sker under hensyntagen til patientens interesse og behov[9].

Det er også tilladt, hvis videregivelsen omfatter et udskrivningsbrev (epikrise) fra en læge ansat i det offentlige sygehusvæsen til patientens alment praktiserende læge eller den praktiserende speciallæge, der har henvist patienten til sygehusbehandling[10].

Hvis patienten har været henvist til behandling på et privat sygehus eller klinik, hvor behandlingen er sket efter aftale med regionen eller kommunen jf. aftalen om det udvidede frie sygehusvalg, skal den læge, der har behandlet patienten på sygehuset eller

[9] Sundhedsloven, §41, stk. 2, nr. 2

[10] Sundhedsloven, §41, stk. 2., nr. 3

klinikken ligeledes sende et udskrivningsbrev(epikrise) til patientens alment praktiserende læge eller den praktiserende speciallæge, der har henvist patienten.

En læge, der har fungeret som stedfortræder for patientens alment praktiserende læge, må videregive oplysninger til den praktiserende læge[11].

Videregivelse af patientoplysninger uden samtykke må herudover ske, hvis det følger af lov, når det er nødvendigt for at varetage en klar almen interesse eller af væsentlige hensyn til patienten, sundhedspersonalet eller andre, f.eks. hvis der er tale om alvorlig smitsom sygdom[12].

I serviceloven[13]findes der bestemmelser om, at kommunalt sundhedspersonale må videregive oplysninger til hinanden eller andre (f.eks. kommunale sagsbehandlere) om børn og unge i forbindelse med konkret forebyggende arbejde. Som udgangspunkt skal udvekslingen ske én gang ved et møde, men i særlige tilfælde kan det også ske på et opfølgende møde. Ligeledes er der i loven[14] mulighed for, at kommunalt sundhedspersonale kan udveksle oplysninger om et barns rent private forhold under behandling af en sag, hvor et børnehus benyttes.

Endelig fastsætter servicelovens § 153 regler om skærpet underretningspligt for visse grupper af offentligt ansatte.

3.1.3 Elektronisk indhentning af patientoplysninger[15]

I modsætning til videregivelse er det ved elektronisk indhentning anvenderen selv, der vurderer hvilke oplysninger, der er nødvendige for den aktuelle behandling og derfor er lovgivningen mere specifik i forhold til, hvilke sundhedspersoner, der må indhente oplysninger.

Læger, tandlæger, jordemødre, sygeplejersker, sundhedsplejersker, social- og sundhedsassistenter, radiografer, kiropraktorer og ambulancebehandlere med særlig kompetence (paramedicinere) må, når det er nødvendigt for den aktuelle behandling,

> Elektronisk indhentning omfatter en sundhedspersons opslag i it-systemer og databaser, der indeholder oplysninger om patientens helbredsforhold, f.eks. elektroniske patientjournaler eller patientadministrative systemer, til brug for patientbehandlingen.

[11] Sundhedsloven, §41, stk. 2, nr. 5

[12] Sundhedsloven, §43

[13] Serviceloven, §49a

[14] Serviceloven, § 50c

[15] Sundhedsloven, §§42a-c samt §§156, 157 og 157a

indhente både historiske og aktuelle oplysninger om patienten på tværs af sektorer og behandlingsenheder.

Aktuelle oplysninger er alle de oplysninger, som er indsamlet i forbindelse med det aktuelle behandlingsforløb, f.eks. en sygehusindlæggelse, tilknytning til hjemmepleje eller tilknytning til et træningscenter.

Med historiske oplysninger menes oplysninger, der ikke er indsamlet i forbindelse med den aktuelle behandling. Det kan altså både være oplysninger fra et andet igangværende behandlingsforløb et andet sted i sundhedsvæsenet og fra et tidligere behandlingsforløb, som er relevant for den aktuelle behandling.

Andre sundhedspersoner end de her nævnte må kun indhente oplysninger om den aktuelle behandling og kun for de patienter, der er på den samme behandlingsenhed, hvor de selv er tilknyttet. Adgangen til oplysningerne skal kunne begrænses teknisk til behandlingsenheden, så man ikke kan slå op på patienter på andre behandlingsenheder[16].

Med udtrykket behandlingsenhed forstås sygehus, sygehusafdeling, afsnit, klinik e.l., og kravet om organisatorisk tilknytning skal datamæssigt administreres så snævert, som det teknisk er muligt[17].

Begrebet behandlingsenhed kan set i lyset af de ændringer, der er sket i sygehusstrukturen i de seneste år, være vanskeligt at fastlægge. Netop derfor er det vigtigt, at der foretages en konkret vurdering af, hvordan det sikres, at der foretages den nødvendige afgrænsning af adgangen for sundhedspersoner, der kun må se oplysninger fra egen behandlingsenhed, så der ikke utilsigtet gives en for bred adgang. Begrebet behandlingsenhed skal fortolkes indskrænket og forudsætter et ansættelsesmæssig tilknytning for sundhedspersonen til enheden.

Datatilsynet har da også i sin afgørelse om adgang til patientjournaler i Region Midtjylland påtalt, at der er givet en meget bred adgang til patientoplysninger.

Sundhedsloven[18] giver mulighed for, at ledelsen på et sygehus eller i en kommune efter en konkret vurdering kan give tilladelse til, at enkelte eller grupper af sundhedspersoner får den samme mulighed for at indhente historiske oplysninger som de ovenfor nævnte grupper, hvis det kræves for at de kan varetage deres funktioner og opgaver. Tilladelsen skal udformes som en datasikkerhedsinstruks og være offentligt tilgængelig, f.eks. på sygehusets hjemmeside.

[16] Sundhedsloven, §42a, stk. 2

[17] Indenrigs- og Sundhedsministeriet: Oversigt over de juridiske rammer for adgangen til EPJ og IT-anvendelsen i sundhedsvæsenet

[18] Sundhedsloven, §42a, stk. 4

Sekretærer (læge- og sygeplejesekretærer) kan under en sundhedspersons ansvar give teknisk hjælp til at indhente oplysninger, som sundhedspersonen selv har adgang til[19].

Ud over indhentning af oplysninger i forbindelse med aktuel behandling åbner sundhedsloven mulighed for, at læger, tandlæger og jordemødre kan indhente oplysninger om patienter, de tidligere har deltaget i behandlingen af, såfremt det har til formål at evaluere egen indsats i forbindelse med behandlingen[20].

Der må også for disse grupper ske indhentning af dokumentation for erhvervede kvalifikationer, hvis der tages hensyn til patientens rettigheder og behov.

Indhentning til brug for evaluering/dokumentation for kvalifikationer skal skeumiddelbart efter at behandlingsforløbet er afsluttet og senest 6 måneder efter, at lægen, tandlægen eller jordemoderen har deltaget i behandlingen. Hvis indhentningen sker som led i speciallæge- eller specialtandlægeuddannelsen, er der ingen tidsbegrænsning.

Formålet med indhentningen skal noteres i patientens journal.

Der gælder særlige og snævrere regler for adgang til det fælles medicinkort og det danske vaccinationsregister[21]. Som udgangspunkt har sundhedspersoner kun adgang til disse registre, når de har patienten i aktuel behandling. Adgang med andre formål kræver altid patientens samtykke.

3.1.4 Samtykke og retten til at frabede sig indhentning eller videregivelse til behandlingsformål[22]

Et samtykke skal være frivilligt, konkret og informeret, og kan i forbindelse med behandling gives enten mundtligt eller skriftligt, både ved videregivelse og elektronisk indhentning[23].

Bevisbyrden for, at der foreligger et samtykke i de situationer, der ikke i medfør af sundhedsloven er undtaget fra kravet om samtykke, ligger hos myndigheden. Det anbefales derfor, at man i disse situationer så vidt muligt indhenter et skriftligt samtykke fra patienten. I situationer, hvor det ikke har været muligt at indhente patientens samtykke, f.eks. på grund af dennes helbredstilstand, bør dette journalføres.

---

[19] Sundhedsloven, §42a, stk 10

[20] Sundhedsloven §42a, stk. 6

[21] Sundhedsloven, §§156, 157 og 157a.

[22] Sundhedsloven §§ 42a og 42b

[23] Sundhedsloven, § 42, stk. 1 og §42b

Patientens samtykke kan ved videregivelse gives til enten den sundhedsperson, der videregiver eller den person, der modtager oplysningerne[24]. Ved indhentning skal tilkendegivelsen ske til den sundhedsperson, under hvis ansvar oplysningerne indhentes[25].

Patientens samtykke skal journalføres både ved videregivelse og indhentning[26].

For det sociale område i kommunerne, er kravet om samtykke til at indhente og videregive oplysninger for andre end autoriserede sundhedspersoner beskrevet i retssikkerhedsloven[27]. Generelt kan kommunen anmode borgere, der søger om hjælp, om at medvirke til at fremskaffe de oplysninger, der er nødvendige for sagens behandling. Adgang til borgerens helbredsoplysninger fra andre myndigheder eller autoriserede sundhedspersoner kræver i alle tilfælde et forudgående samtykke fra borgeren.

3.1.4.1. Retten til at frabede sig indhentning eller videregivelse

Forudsætningen for at kunne videregive og indhente helbredsoplysninger i forbindelse med aktuel behandling uden patientens konkrete samtykke er, at patienten er blevet gjort bekendt med, at han har mulighed for at frabede sig, at hans oplysninger videregives[28] eller indhentes[29].

Patienten kan enten mundtligt eller skriftligt frabede sig at oplysninger videregives eller indhentes[30]. Patientens tilkendegivelse kan ske til enten den sundhedsperson, der videregiver eller den person, der modtager oplysningerne[31].

Ved indhentning skal tilkendegivelsen ske til den sundhedsperson eller under hvis ansvar oplysningerne indhentes[32].

Patientens tilkendegivelse skal journalføres både ved videregivelse og indhentning[33].

---

[24] Sundhedsloven, § 42, stk. 1

[25] Sundhedsloven, § 42b

[26] Sundhedsloven, § 42, stk. 1 og §42b

[27] Retssikkerhedsloven, §§ 11-11a

[28] Sundhedsloven, § 41, stk. 3

[29] Sundhedsloven, § 42a, stk. 8

[30] Sundhedsloven, § 42, stk. 1 og §42b

[31] Sundhedsloven, § 42, stk. 1

[32] Sundhedsloven, § 42b

[33] Sundhedsloven, § 42, stk. 1 og §42b

Patienten skal informeres om konsekvenserne ved at frabede sig videregivelse og/eller indhentning af oplysninger ved aktuel behandling, og det anbefales at det tydeligt fremgår af skærmbillede eller papirjournal, at patienten har frabedt sig videregivelse og/eller indhentning af oplysninger.

3.1.5 Værdispringsreglen

Værdispringsreglens oprindelige grundlag findes i forvaltningsloven[34]. Efter denne regel er en forvaltningsmyndighed berettiget til at give følsomme oplysninger videre til en anden myndighed uden borgerens samtykke, når der er et klart værdispring mellem på den ene side hensynet til de interesser, der begrunder hemmeligholdelsen selv over for andre myndigheder, og på den anden side afgørende modhensyn til enten private eller offentlige interesser. Serviceloven opererer på samme grundlag.

Der er tale om en regel, der rent undtagelsesvis tages i anvendelse.

For sundhedsvæsenet er det primært sundhedslovens regler vedr. værdispring[35], der anvendes. Værdispringsreglen kan anvendes ved videregivelse eller indhentning af oplysninger til den aktuelle patientbehandling, hvis der er hensyn til patienten selv, medarbejderne eller samfundet som helhed, der overstiger vedkommendes interesse at hemmeligholde oplysningerne.

Formålet er primært at sikre, at en sundhedsperson ikke kommer i en situation, hvor vedkommende mangler vigtig patientinformation, f.eks. hvis patienten er bevidstløs og ikke kan besvare evt. spørgsmål, og dermed påfører patienten en risiko.

Et andet eksempel, som fremgår af forarbejderne til loven, er at en sundhedsperson har behov for at tilgå en journal for at indhente oplysninger om et sammenligneligt tilfælde i behandling af sjældent forekommende, alvorlig sygdom. Her overstiger hensynet til den aktuelle patientbehandling den enkelte patients krav på fortrolighed.

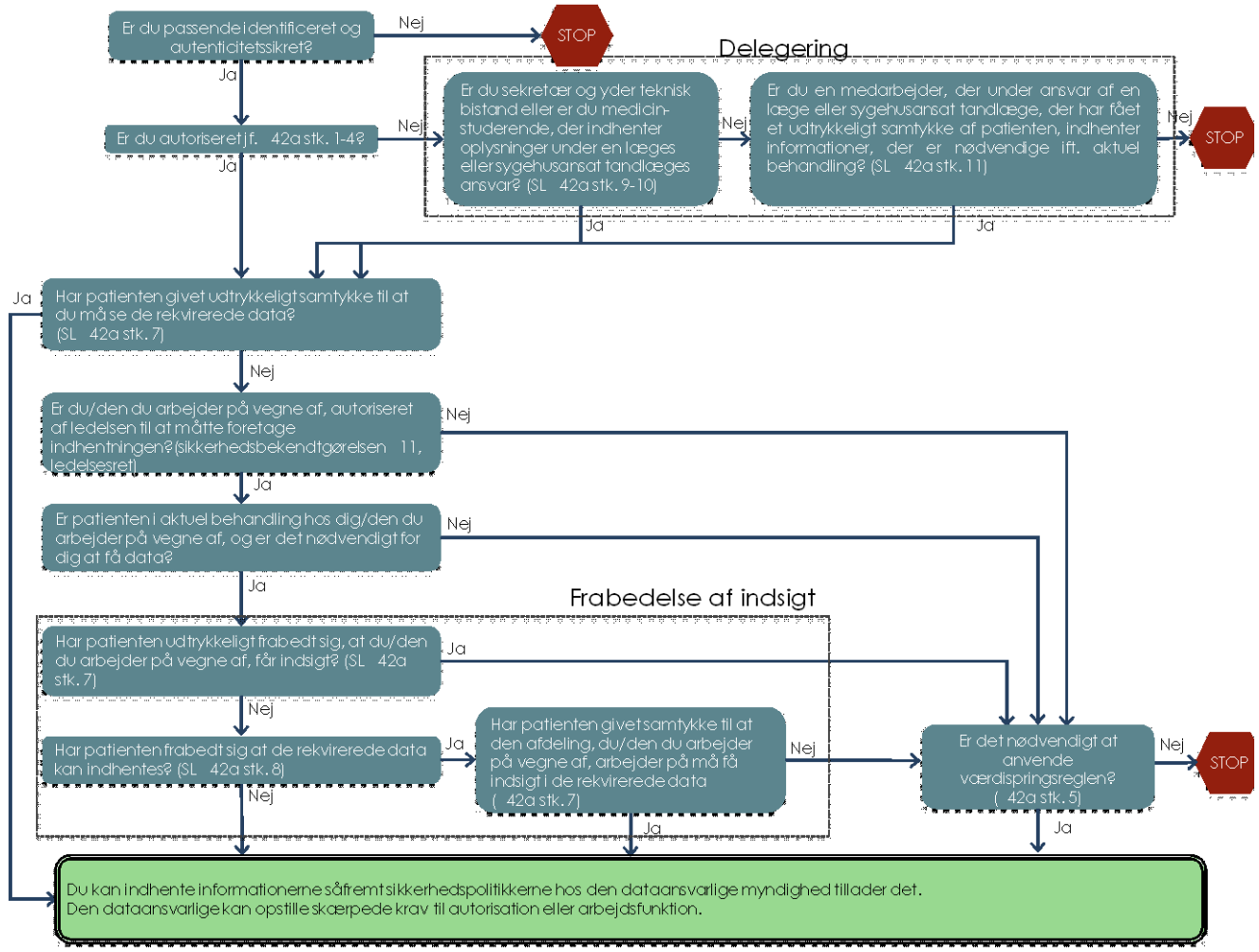
På den anden side er det vigtigt, at værdispringsreglen ikke anvendes til at omgå eksisterende sikkerhedsløsninger eller anden lovgivning, og det er derfor vigtigt, at der er foretaget en konkret vurdering, hvor formålet med at anvende reglen overstiger hensynet til patienten væsentligt. Endvidere er det vigtigt, at der er hos myndigheden er fastsat klare regler for dokumentation og opfølgning på anvendelsen.

3.1.6 Beslutningsgraf vedr. sundhedspersoners elektroniske indhentning af patientoplysninger

I nedenstående figur er de forskellige bestemmelser sat op som en beslutningsgraf, der bidrager til at tydeliggøre, hvornår man må, og hvornår man ikke må indhente oplysninger elektronisk.

[34] Forvaltningsloven, §28, stk. 2, nr.3

[35] Sundhedsloven, §41, stk. 2 (videregivelse) og §42a, stk. 5 (elektronisk indhentning)



Figur 2: Beslutningsgraf vedr. sundhedspersoners indhentning af patientoplysninger (Kilde: Referencearkitektur for informationssikkerhed, NSI 2013, revideret i forhold til ændringer i sundhedslovens §42a)

3.2 Sekundær anvendelse af helbredsoplysninger[36]

Patientoplysninger anvendes ikke kun i den direkte patientbehandling, men indgår som grundlag for administration, ledelsesinformation, afregning, planlægning, kvalitetssikring og forskning.

> Sekundær anvendelse af helbredsdata dækker alle andre formål end direkte patientbehandling.

Med patientens samtykke kan sundhedspersoner til andre formål end behandling videregive oplysninger om patientens helbredsforhold, øvrige rent private forhold og andre fortrolige oplysninger til sundhedspersoner, myndigheder, organisationer, private personer m.fl. Patienten skal orienteres om formålet med videregivelsen.

[36] Sundhedsloven, §§43-44

Samtykke er gyldigt i et år og skal journalføres.

Uden samtykke er det tilladt at videregive oplysninger når:

- det følger af lov eller bestemmelser, at oplysningen skal videregives og oplysningen må antages at have væsentlig betydning for den modtagende myndigheds sagsbehandling, f.eks. lægers pligt til at indberette i sociale sager, ved dødsfald eller ved pålæg fra domstolene
- videregivelsen er nødvendig for berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, sundhedspersonen eller andre, f.eks. hvis patienten lider af en smitsom sygdom
- videregivelsen er nødvendig for, at en myndighed kan gennemføre tilsyns- og kontrolopgaver, f.eks. opfølgning i forhold til afregning af ydelser i praksissektoren[37].

3.2.1 Administration, herunder ledelsesinformation og afregning

Til administrative formål, der indebærer behandling af personhenførbare oplysninger gælder det i sundhedsloven, at man med patientens samtykke må videregive helbredsoplysninger til andre formål til andre myndigheder, organisationer og private personer. Dog kræves der ikke samtykke, hvis det af anden lovgivning fremgår, at en sundhedsperson eller myndighed har pligt til at videregive oplysningerne, f.eks. indberetning af smitsomme sygdomme eller indberetning til Landspatientregisteret[38], jf. ovenstående oversigt.

Af retssikkerhedsloven[39] fremgår, at kommuner og sygehuse uden samtykke må udveksle oplysninger om indlæggelse og udskrivning af borgere i kommunen (advis) med henblik på planlægning af ydelser for borgeren.

Som udgangspunkt må der ikke være personoplysninger i systemer til planlægning og ledelsesinformation, idet der ikke er hjemmel i sundhedsloven til, at patientoplysninger fra patientbehandlingssystemerne kan overføres til planlægnings- og ledelsesinformationssystemer uden den enkelte patients samtykke.

[37] Sundhedsloven, §43, stk. 2

[38] Sundhedsloven, §46, §157 (FMK), 157a (DDV), §195 (f.eks. LPR)

[39] Retssikkerhedsloven, §12c

Med ændringen af sundhedsloven i 2011[40] fik kommuner og regioner adgang til eSundhed.dk med henblik på planlægning og tilrettelæggelse af indsatsen på sundhedsområdet jf. sundhedslovens § 197. Bestemmelsen indebærer, at administrative medarbejdere i regioner og kommuner må behandle oplysninger på personniveau, dette med henblik på at kunne udarbejde statistiske undersøgelser til brug for planlægning, tilrettelæggelse, analyse og evaluering.

> eSundhed er en portal, hvor man kan få adgang til sundhedsdata på regions-, hospitals- og kommunalt niveau. Der findes en version, hvor alle kan se aggregerede data, og en lukket version, der kan anvendes af medarbejder i regioner og kommuner.

Oplysningerne må alene anvendes i statistisk øjemed. Det indebærer, at de ikke må bruges til konkret regningskontrol og heller ikke i den konkrete sags- eller patientbehandling. Hjemlen er endnu ikke udmøntet i en bekendtgørelse, der nærmere fastsætter retningslinjer for anvendelsen.

Med baggrund i sundhedslovens § 195 om indberetning til centrale sundhedsmyndigheder og cirkulærer om statens tilskud til regionernes sygehusvæsen og kommunernes medfinansiering er det lovfæstet, at personhenførbare oplysninger vedr. sygehusbehandling, behandling i speciallægepraksis og behandling på private sygehuse og klinikker skal indberettes til Sundhedsdatastyrelsen med henblik på at

> DRG-systemet er et redskab til at gruppere patienter i Diagnose Relaterede Grupper. DRG bruges til at give et billede af sammenhængen mellem aktivitet og udgift for forskellige behandlingstyper og ligger til grund for beregning af de takster, der bruges til afregning mellem regionerne og kommunerne.

dokumentere aktiviteten og danne grundlag for gruppering i DRG- eller DAGS-grupper, som anvendes til afregning mellem parterne.

I forhold til praksissektorens afregning med Regionernes lønnings- og takstnævn er det sundhedslovens § 43, stk. 2, nr. 3 om myndigheders kontrol og tilsyn, der regulerer videregivelsen af oplysninger.

Herudover er der i sundhedslovens § 228 regler for afregning med sundhedspersoner, der ikke er omfattet af en overenskomst.

[40] Sundhedslove, §195

3.2.2 Kliniske kvalitetsdatabaser

Efter sundhedslovens § 196 har sundheds og ældreministeren mulighed for at fastsætte regler for indberetning til og behandling af data i af Sundhedsdatastyrelsen godkendte kliniske landdækkende eller regionale kvalitetsdatabaser med henblik på overvågning og udvikling af behandlingsresultater. Disse bestemmelser fremgår af bekendtgørelsen om indberetning af oplysninger til de kliniske kvalitetsdatabaser m.v.

> Kliniske kvalitetsdatabaser bruges til opfølgning og kvalitetssikring på behandlingsresultaterne. Opfølgningen er baseret på de kliniske indikatorer, der er fastlagt for den enkelte database.

Der kræves ikke samtykke fra patienten til indberetning til en godkendt klinisk kvalitetsdatabase og behandling af data fra disse databaser.

I forbindelse med kvalitetssikringen af data i de godkendt kliniske kvalitetsdatabaser kan der være behov for, at sundhedspersoner hos den myndighed, der indberetter til databasen, kan tilgå deres eget patientregistreringssystem, elektroniske patientjournal eller en papirjournal for at kontrollere, at de indberettede oplysninger er korrekte.

Der er ikke i bekendtgørelsen om de kliniske kvalitetsdatabaser angivet andet, end at den dataansvarlige myndighed er ansvarlig for, at databasen lever op til kravene i bekendtgørelsen, men da der er tale om en lovhjemlet kontrolopgave, kan sundhedspersoner indhente de nødvendige oplysninger og videregive disse til den ansvarlige for kvalitetsdatabasen[41].

3.2.3 Videnskabelige og statistiske undersøgelser[42]

I sundhedsloven findes regler om sundhedspersoners videregivelse af oplysninger til forskning og statistik. Det er sundhedsperson, der har ansvaret for de registrerede oplysninger, der må videregive oplysninger til videnskabelige eller statistiske formål.

Det vil sige, at forskeren ikke selv elektronisk må indhente oplysninger i f.eks. patientjournaler eller i Sundhedsjournalen e.l. med henblik på at lave videnskabelige eller statistiske undersøgelser.

[41] Sundhedsloven, §43, stk. 2, pkt. 3

[42] Sundhedsloven, § 46

Den, der har ansvaret for de oplysninger, der skal videregives til videnskabelige eller statistiske formål, kan være nødt til at indhente data i de databaser, hvor de er placeret. Denne opgave kan dog i henhold til autorisationslovens bestemmelser om delegation43 overdrages til en betroet medarbejder eller en sekretær, der yder teknisk bistand, under den pågældende sundhedspersons ansvar. Hvis opgaven delegeres, vil det være hensigtsmæssigt at dokumentere, med hvilket formål oplysningerne er indhentet.

Sundhedsjournalen indeholder oplysninger om borgernes behandlinger, medicin, lægemiddelallergier m.m. Sundhedspersoner, der har en aktuel behandlingsrelation og borgerne selv har adgang til oplysningerne.

3.2.3.1 Klinisk forskning

Oplysninger fra patientjournaler kan videregives uden patientens samtykke til brug for et konkret sundhedsvidenskabeligt forskningsprojekt[44], såfremt der er indhentet tilladelse til projektet fra en videnskabsetisk komité.

Dette er relevant, når en forsker forinden inklusion af deltager skal bruge oplysninger fra patientjournaler til at screene mulige deltagere til klinisk forskning. Det vil være et krav, at screeningsproceduren og den efterfølgende rekrutteringsprocedure er beskrevet tydeligt i den protokol, der forelægges til vurdering for den videnskabsetiske komité. Den fortsatte brug af patientjournaler i det kliniske forsøg efter inklusion af deltagerne forudsætter, at deltagerne er informeret herom i deltagerinformationen.

Det følger desuden af komitéloven[45], at et samtykke fra en forsøgsdeltager i et sundhedsvidenskabeligt forskningsprojekt medfører, at der kan videregives nødvendige oplysninger fra deltagerens patientjournal mv., til en sponsor eller monitor (fx en GCP-enhed), som gennemfører lovpligtig egenkontrol, herunder kvalitetskontrol og monitorering af forsøget.

Herudover kan en videnskabsetiske komité få videregivet og behandle nødvendige oplysninger fra patientjournaler som led i komiteens videnskabsetiske tilsyn med et godkendt projekt[46].

[43] Autorisationsloven, §18 fastsætter regler om, at en autoriseret sundhedsperson kan delegere alle former for forbeholdt sundhedsfaglig virksomhed til en medhjælp. Der er udfærdiget en negativliste, dvs. hvad der ikke kan delegeres. Opslag i elektroniske systemer er ikke på negativlisten.

[44] Sundhedsloven, §46, stk. 1

[45] Komiteloven, §3, stk 3

[46] Komiteloven, §29

I kliniske forsøg med lægemidler gælder tilsvarende for Lægemiddelstyrelsens inspektører. I kliniske lægemiddelforsøg er det almindeligt, at forsøgsdeltagerne bliver bedt om at underskrive en fuldmagt til, at oplysninger fra deltagernes patientjournal videregives til udenlandske tilsynsmyndigheder (fx FDA), til brug for nødvendig kvalitetskontrol af oplysningerne.

Inklusion af forsøgspersoner i klinisk forskning kræver altid forudgående samtykke (med undtagelse af forskning i akutte forsøgssituationer i forsøg, der ikke vedrører afprøvning af lægemidler).

Kravet om samtykke gælder som udgangspunkt også ved forskning i biologisk materiale, der allerede er udtaget fra patienter og befinder sig i en klinisk biobank, eller er udtaget i forbindelse med et tidligere forskningsprojekt og opbevares lovligt (med Datatilsynets tilladelse). Det er dog muligt at søge en videnskabsetisk komité om dispensation fra kravet om samtykke, hvis forskningen ikke indebære risici eller på anden måde i øvrigt kan være til belastning for forsøgspersonen[47].

Ved udlevering af biologisk materiale fra en klinisk biobank til brug for et godkendt sundhedsvidenskabeligt forskningsprojekt skal den biobankansvarlige sundhedsperson sikre sig, at de pågældende patienter ikke har registreret et forbehold mod forskningsmæssig brug i vævsanvendelsesregistret[48]

3.2.3.2 Anden forskning med udgangspunkt i patientjournaler

Hvis oplysninger fra patientjournaler skal bruges til et konkret forskningsprojekt, der ikke er omfattet af reglerne for behandling af sundhedsvidenskabelige forskningsprojekter (komitéloven), skal Styrelsen for Patientsikkerhed give tilladelse til videregivelsen. Dette vil være tilfældet ved rene registerforskningsstudier, hvor der ikke inddrages menneskeligt biologisk materiale eller undersøgelser af mennesker.

En forsker må kun rette henvendelse til enkeltpersoner på grundlag af oplysningerne i patientjournalen, såfremt den sundhedsperson, der har behandlet patienten, har givet tilladelse hertil[49]. Dette gælder både for forskning godkendt af en videnskabsetiske komité eller af Styrelsen for Patientsikkerhed. Tilladelse fra behandlende sundhedsperson kan fx være relevant for forskere, der anvender oplysninger fra (elektroniske) patientregistre til at fremfinde egnede deltagere til et klinisk forskningsprojekt eller en spørgeskemaundersøgelse.

3.2.4 Videregivelse og oplysninger til tilsynsmyndigheder og til behandlingen af klage- og erstatningssager

Hvis en sundhedsperson, der er klaget over, ønsker at få adgang til journalmateriale, der findes i andre organisationers elektroniske systemer, eksempelvis på sundhed.dk,

[47] Komiteloven, § 10

[48] Sundhedsloven, § 29, stk. 4

[49] Sundhedsloven, §46, stk. 3

kan dette alene ske med patientens samtykke. Hvis ikke det er muligt at få patientens samtykke, må den indklagede sundhedsperson rette henvendelse til klagemyndigheden, der herefter må sende sundhedspersonen det manglende journalmateriale, der ses at være relevant for klagesagen.

Hvis en autoriseret sundhedsperson eller et sygehus bliver indklaget i en klagesag anlagt ved Styrelsen for Patientsikkerhed[50] (enten som en klage over en konkret sundhedsperson, som afgøres af Sundhedsvæsenets Disciplinærnævn[51], eller som en klage over behandlingsstedet, der afgøres af Styrelsen for Patientsikkerhed[52]) eller Patienterstatningen[53], vil der i medfør af lov om klage- og erstatningsadgang i sundhedsvæsenet være pligt til at videregive oplysninger til henholdsvis Styrelsen for Patientsikkerhed, Sundhedsvæsenets Disciplinærnævn og Patienterstatningen.

I medfør af lov om klage- og erstatningsadgang i sundhedsvæsenet, jf. sundhedsloven, vil der således være hjemmel til, at der kan foretages opslag i sundhedspersonens eller sygehusets **egne** systemer for så vidt angår optegnelser over den behandling, der er klaget over, til brug for varetagelse af sundhedspersonens/sygehusets interesser i klagesagen.

3.2.5 Videregivelse til politiet

Sundhedslovens bestemmelser regulerer, hvornår der lovligt med anvendelse af værdispringsregelen at videregive oplysninger fra patientjournaler til politiet ved efterforskning af alvorlig kriminalitet som manddrab, seksualforbrydelser, grov vold mv, herunder vold mod børn[54].

Politiets adgang til oplysninger om enkeltpersoner fra andre kilder, f.eks. sundhedsdataregistre, er reguleret i retsplejelovens kapitel 74 om beslaglæggelse og edition. Politiet må herefter som udgangspunkt kun få adgang til borgeres helbredsoplysninger, såfremt der foreligger en dommerkendelse.

---

[50] En af de opgaver, som Styrelsen for Patientsikkerhed varetager, er at afgøre klager over tilsidesættelse af patientrettigheder og klager over sundhedsfaglig behandling, hvor en eventuel kritisk ønskes rettet mod behandlingsstedet og ikke mod en konkret sundhedsperson. Derudover er Styrelsen for Patientsikkerhed også sekretariat for Sundhedsvæsenets Disciplinærnævn, der behandler klager over konkrete sundhedspersoners sundhedsfaglige behandling.

[51] Lov om klage- og erstatningsadgang inden for sundhedsvæsenet, § 16, stk. 1, jf. sundhedslovens § 43, stk. 1.

[52] Lov om klage- og erstatningsadgang inden for sundhedsvæsenet, § 12, stk. 2, jf. sundhedslovens § 43, stk. 1.

[53] Lov om klage- og erstatningsadgang inden for sundhedsvæsenet, § 37, stk. 1, jf. sundhedslovens § 43, stk. 1.

[54] Sundhedsloven, § 43, stk. 2, nr. 2

3.2.6 Andet[55]

Patienternes oplysning kan videregives til andre formål end de ovenfor beskrevne, men det kræver altid patientens skriftlige samtykke. Kravet om skriftlighed kan dog fraviges, når sagens karakter eller omstændighederne i øvrigt taler derfor.

Det kræver således et konkret samtykke, hvis man vil videregive oplysninger til forsikringsselskaber, arbejdsgiver, pensionsselskaber o.l. Som udgangspunkt skal samtykket være skriftlige, men kan afhængigt af omstændigheder være mundtligt.

Samtykke skal journalføres og bortfalder efter 1 år[56].

3.2.7 Tilbagekaldelse af samtykke

Samtykke kan tilbagekaldes af patienten, hvorved enhver videregivelse af oplysninger, der har været tilladelse til på baggrund af samtykket, skal stoppe øjeblikkelig. Det påhviler den dataansvarlige myndighed at sikre at det dels er teknisk muligt at stoppe videregivelse af oplysninger, dels findes en proces for organisatorisk at håndtere, at videregivelsen stoppes.

3.2.8. Videregivelse til andre – offentlighedsloven

Jf. offentlighedsloven har enhver har ret til aktindsigt med de begrænsninger, der følger af loven, herunder at der ikke er ret til aktindsigt i helbredsoplysninger[57].

[55] Sundhedsloven, §§ 43-44

[56] Sundhedsloven, §44

57 Offentlighedsloven, §30 https://www.retsinformation.dk/forms/r0710.aspx?id=152299

4. Dataansvar

Persondataloven sætter rammerne for, hvordan offentlige myndigheder, private virksomheder, forskere mv. skal håndtere personoplysninger. Man skal være opmærksom på, at begrebet "behandling" ikke har noget med patientbehandling at gøre, men dækker over forskellige måder at håndtere personoplysninger på: indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse, transmission, formidling, sammenstilling, samkøring, blokering og sletning[58].

Persondataloven opererer med rollerne: den dataansvarlige[59] og databehandleren[60].

Den dataansvarlige er den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger. Databehandleren er den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.

[58] Persondataloven, §3, stk. 2

[59] Persondataloven, §3, stk. 4

[60] Persondataloven. §3, stk.5

4.1 Den dataansvarliges forpligtelser

Den dataansvarlige er den person eller myndighed, der er ansvarlig for, at persondatalovens krav overholdes i forbindelse med behandling af personoplysninger. Det indebærer bl.a., at det er den dataansvarlige, der har pligt til at anmelde databehandlingen til Datatilsynet, når det er påkrævet (se kapitel 4.4 vedr. undtagelser fra anmeldelsespligten), sikre, at borgerens rettigheder tilgodeses og som har ansvaret for, at der etableres de fornødne tekniske og organisatoriske sikringsforanstaltninger, som f.eks. brugerstyring, logning m.v. Disse sikringsforanstaltninger skal sikre, at oplysningerne ikke hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, at oplysningerne ikke kommer til uvedkommendes kendskab eller misbruges, eller at oplysningerne behandles i strid med persondataloven.

> Den dataansvarlige er defineret som den fysiske eller juridiske person, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af de pågældende personoplysninger.

Konkret kan en dataansvarlig være en offentlig myndighed: styrelse, region eller kommune, der registrerer oplysninger, der er nødvendige for at kunne udføre de opgaver, myndigheden har ansvaret for. Men det kan også være en praktiserende læge, der behandler patientoplysninger i forbindelse med sin praksis m.v. eller en sundhedsperson, der ikke er ansat hos en offentlig myndighed, men foretager videnskabelige eller statistiske undersøgelser med brug af patientoplysninger.

Offentlige myndigheder er som dataansvarlige forpligtet til at efterleve bekendtgørelsen om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, i daglig tale kaldet sikkerhedsbekendtgørelsen. Sikkerhedsbekendtgørelsen indeholder bestemmelser om, hvilke sikringstiltag, der skal etableres, når der behandles personoplysninger.

For private virksomheder, herunder privatklinikker og privatpraktiserende læger er der ikke krav om at efterleve sikkerhedsbekendtgørelsens bestemmelser, men som det fremgår af vejledningen til sikkerhedsbekendtgørelsen, gælder persondatalovens bestemmelser umiddelbart. Datatilsynet anbefaler dog, at private aktører efterlever sikkerhedsbekendtgørelsens bestemmelser, ligesom der ved akkreditering af almen praksis er et krav om, at klinikkerne kan leve op til kravene i sikkerhedsbekendtgørelsen.

Eftersom der ikke er lovmæssigt krav til private sundhedsaktører om at efterleve sikkerhedsbekendtgørelsen, anbefales det, at offentlige myndigheder, der indgår aftale med private klinikker, sygehuse o.l., sikrer sig, at krav til informationssikkerhed skrives ind i aftalen**,** dog således, at der tages hensyn til, at der generelt er tale om mindre virksomheder, og der skal være proportionalitet mellem krav til sikkerhed og de dermed forbundne omkostninger.

I det omfang en privat sundhedsorganisation handler som databehandler for en offentlig myndighed, gælder sikkerhedsbekendtgørelsen dog også for behandlingen af

personoplysninger hos databehandleren, hvilket også skal fremgå af den skriftlige databehandleraftale (se kapitel 4.3).

For nogle databehandlinger, f.eks. Sundhedsjournalen på sundhed.dk eller Mikrobiologidatabasen, er de enkelte regioner dataansvarlige for egne oplysninger og ansvarlige for hver for sig at indgå en databehandleraftale med den fælles databehandler.

Indsamling af personoplysninger må kun ske til saglige formål, dvs. at indsamlingen skal være begrundet i løsning af en opgave, som myndigheden har ansvaret for. Man må ikke ved senere behandling anvende oplysningerne til formål, der er uforenelige med det oprindelige formål, hvortil oplysningerne er indsamlet[61] eller i strid med anden lovgivning.

Oplysninger kan videregives til andre dataansvarlige, hvis patienten har givet samtykke, det er lovpligtigt, hvis der er hjemmel hertil i persondataloven eller anden lovgivning og formålet med videregivelsen i øvrigt er saglig og relevant. Derudover må formålet med behandlingen hos den nye dataansvarlige ikke være uforeneligt med det oprindelige formål med indsamlingen. Den dataansvarlige er ligeledes ansvarlig for, at der ikke behandles urigtige eller vildledende oplysninger. Hvis det viser sig, at der er registreret urigtige eller vildledende oplysninger, skal disse berigtiges, slettes eller blokeres[62].

4.2 Hjemmel til behandling af oplysninger

Enhver behandling af personoplysninger i sundhedsvæsenet skal have en hjemmel i lovgivningen, med mindre borgeren har givet samtykke til behandlingen. Hjemmel er den lovparagraf, der indeholder bestemmelser om, hvordan opgaven skal løses. Mange gange vil hjemlen være uddybet i en bekendtgørelse til loven.

I det omfang, behandlingen af personoplysninger ikke er reguleret af særlovgivning, finder persondatalovens regler anvendelse.

Hjemmel til indsamling og registrering i patientjournaler skal primært findes i autorisationsloven og journalføringsbekendtgørelsen, hvoraf det fremgår, at enhver autoriseret sundhedsperson, som foretager behandling af en patient, skal føre en patientjournal pr. patient[63]

For hver patient oprettes én patientjournal på hvert enkelt sygehus, klinik, praksis, kommunalt sundhedscenter, bosted mv. I det offentlige sundhedssystem kan der for hver patient oprettes en patientjournal for hver region, når der er teknisk mulighed for det[64].

[61] Persondataloven, §5

[62] Persondataloven, §37

[63] Journalføringsbekendtgørelsen, §§ 2-3

[64] Journalføringsbekendtgørelsen §3

Herudover indeholder sundhedsloven hjemmelsbestemmelser for det fælles medicinkort (FMK)[65] og det danske vaccinationsregister (DDV)[66], det nationale patientindeks[67], landsdækkende og regionale kliniske kvalitetsdatabaser[68] og planlægning af indsatsen på sundhedsområdet.

Det fremgår af § 157 i sundhedsloven, at Sundhedsdatastyrelsen er ansvarlig for at drive en elektronisk registrering af de enkelte borgeres medicinoplysninger, herunder ordination, køb, udlevering, indtagelse, dosisændring, ophør og sundhedspersoners instruktioner om brug af medicin, samt oplysninger, der er relateret til borgernes medicinoplysninger (FMK) På samme måde er Statens Seruminstitut efter §157a i sundhedsloven ansvarlig for at drive en elektronisk registrering af oplysninger om de enkelte borgeres vaccinationer (DDV).

I sundhedslovens § 193b bemyndiges ministeren til at udpege en myndighed, der er dataansvarlig for et elektronisk indeks (Nationalt Patientindeks) over registreringer af de enkelte borgeres helbredsoplysninger, herunder medicinoplysninger, vaccinationsoplysninger, journaloplysninger, laboratoriesvar m.v. Denne hjemmel i sundhedsloven gælder i modsætning til de ovennævnte § 157 og §157a ikke en konkret eksisterende løsning.

Det fremgår af sundhedslovens § 196, at Sundhedsdatastyrelsen godkender landsdækkende og regionale kliniske kvalitetsdatabaser, som en offentlig myndighed er dataansvarlig for. Sundhedsdatastyrelsen fastsætter nærmere regler for procedure og kriterier for godkendelse af kliniske kvalitetsdatabaser og for kvalitetsdatabasernes virke.

Af sundhedslovens § 197 fremgår det, at regionsrådene og kommunalbestyrelserne til brug for tilrettelæggelse og planlægning af den regionale indsats på sundhedsområdet kan indhente og behandle personoplysninger fra offentlige registre om patienters modtagelse af sundhedsydelser. Der mangler imidlertid endnu en udmøntning af bestemmelsen i en bekendtgørelse, før den kan ibrugtages.

Herudover er der specifikke hjemmelsbestemmelser i sundhedslovens § 198 om patientsikkerhed, hvoraf det fremgår, at regionsrådet og kommunalbestyrelsen modtager, registrerer og analyserer rapporteringer om utilsigtede hændelser, til brug for forbedring af patientsikkerheden og rapportering af oplysninger til Styrelsen for Patientsikkerhed[69].

[65] Sundhedsloven, § 157

[66] Sundhedsloven, § 157a

[67] Sundhedsloven, § 193b

[68] Sundhedsloven, § 196

[69] Sundhedsloven, §199

I forbindelse med registerforskning (defineret som videnskabelige eller statistiske undersøgelser, der alene bygger på oplysninger fra landsdækkende registre eller andre registre, der ikke er patientbehandlingssystemer) findes hjemlen til behandling af personoplysninger ikke i sundhedsloven, men kan evt. findes i persondatalovens § 10.

4.3 Databehandlere

En dataansvarlig kan vælge at overlade det til en ekstern part at udføre selve den praktiske behandling af personoplysninger på den dataansvarliges vegne, som så betegnes som databehandler.

Det skal bemærkes, at man kun anvender begrebet databehandler, når der er tale om en ekstern part, der foretager databehandlinger på vegne af en dataansvarlig. Selv om den dataansvarlige selv varetager databehandling, anvendes begrebet databehandler ikke.

En databehandler må kun behandle personoplysninger på vegne af og efter instruks fra en dataansvarlig. Databehandleren må ikke behandle personoplysninger til egne formål og må derfor ikke bruge de overladte oplysninger til andet end udførelsen af opgaven for den dataansvarlige.

En databehandler er en fysisk eller juridisk person, offentlig myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne.

I praksis kan en databehandler være en virksomhed, som drifter en anden virksomheds eller en offentlig myndigheds IT-systemer. På sundhedsområdet kan som eksempel nævnes, at MedCom fungerer som databehandler for sundhedsvæsenets parter i forbindelse med drift af Sundhedsdatanettet. Et andet eksempel er sundhed.dk, der er databehandler for regioner, kommuner og statslige myndigheder i forhold til en lang række tjenester, f.eks. Sundhedsjournalen. Endelig er der en række private leverandører, der er databehandlere for forskellige aktører i sundhedsvæsenet, f.eks. er CGI databehandler for Sundhedsdatastyrelsen i forbindelse med driften af Landspatientregisteret.

En databehandler kan også være en leverandør, der alene har adgang til oplysninger for at varetage en supportfunktion i forhold til brugerne af en it-løsning.

Den dataansvarlige skal indgå en skriftlig aftale med databehandleren, som bl.a. indeholder oplysninger om, hvilke databehandlinger, databehandleren varetager for den dataansvarlige og de konkrete vilkår, det foregår under.

Hvis der anvendes eksterne konsulenter i forbindelse med drift af systemer i organisationens eget it-miljø, og disse konsulenter kan få adgang til personoplysninger, skal der ligeledes udarbejdes en databehandleraftale.

Såfremt der er flere dataansvarlige, jf. ovenfor, hvor regionerne hver især er ansvarlige for egne data, er der behov for, at der er konsensus om den databehandleraftale, der indgås med databehandleren. Det kan være hensigtsmæssigt, at de dataansvarlige etablerer en styregruppe e.l., der kan agere på vegne af alle over for databehandleren. Hermed kan det sikres, at evt. supplerende krav til databehandleren, f.eks. som følge af lov- eller revisionsmæssige krav, koordineres, eftersom databehandleren ikke, hvis der er tale om samme database, kan efterkomme forskellige sikkerhedshensyn fra de forskellige dataansvarlige.

Når ordlyden i databehandleraftalen er forhandlet på plads, skal hver dataansvarlige myndighed underskrive en individuel databehandleraftale, hvori kun den dataansvarlige myndighed og databehandleren er parter.

4.3.1 Indholdet af den skriftlige databehandleraftale

Den skriftlige aftale imellem den dataansvarlige og databehandleren skal bl.a. indeholde bestemmelse om, at databehandleren alene handler efter instruks fra den dataansvarlige og at der skal etableres de nødvendige sikringsforanstaltninger.

Generelt bør der indgås en mere detaljeret databehandleraftale, når der er tale om større og eventuelt mere komplicerede løsninger, der indeholder fortrolige eller følsomme oplysninger. Dette for at sikre, at myndighedens eller virksomhedens forpligtelse til at beskytte oplysningerne bliver opfyldt også ved behandlingerne hos databehandleren.

Den dataansvarlige skal sikre sig, at databehandleren træffer de nødvendige tekniske og organisatoriske sikringsforanstaltninger og aktivt påse, at disse overholdes hos databehandleren. I den sammenhæng kan det være relevant at fremsende relevant dokumentation for sikringsforanstaltninger, fx en årlig revisionserklæring eller en anden uvildig erklæring fra relevant person med speciale/certificering i it-sikkerhed. Databehandleraftalen bør indeholde krav om adgang til en uvildig erklæring som en betingelse for at lade behandlingen foretage hos databehandleren.

Hvis der i forbindelse med anvendelsen af f.eks. medicoteknisk udstyr behandles personoplysninger, kan der ligeledes være behov for udarbejdelse af en skriftlig databehandleraftale.

Som bilag til aftalen kan der laves en konkret databehandlerinstruks. Databehandlerinstruksen skal konkret og tilstrækkeligt detaljeret beskrive krav til databehandlerens sikringsforanstaltninger.

Databehandlerinstruksen skal beskrive krav til:

- Autentificering og adgangskontrol
- Fysisk sikring
- Evt. krav om logning
- Logopfølgning/audit
- Kryptering

- Håndtering af uddatamateriale
- Rekvirering af auditlog
- Procedurer for håndtering af sikkerhedshændelser (ISO 27001)

Databehandlerinstruksen kan være indarbejdet i databehandleraftalen eller den kan erstattes af, at databehandleren skriver under på, at de følger de samme retningslinjer, som er gældende hos den dataansvarlige selv.

I forhold til eventuelle underdatabehandlere skal den dataansvarlige myndighed enten indgå en databehandleraftale direkte med en underdatabehandler, eller databehandleren skal have fundmagt til på vegne af den dataansvarlige myndighed at indgå en databehandleraftale med dennes underdatabehandler.

4.4 Anmeldelse til Datatilsynet.

Visse behandlinger af fortrolige og følsomme personoplysninger skal anmeldes til Datatilsynet. Formålet er at kunne kontrollere, at databehandlingen lever op til reglerne i persondataloven og sikre gennemskuelighed i forhold til behandlinger af personoplysninger.

Det skal understreges, at anmeldelsesordningen ikke ændrer på, at det er den dataansvarlige myndighed, der skal sikre, at lovens regler overholdes. Dette gælder også, selvom en databehandling er undtaget fra anmeldelse.

For offentlige myndigheder har Datatilsynet på visse nærmere afgrænsede områder udarbejdet såkaldte paraplyanmeldelser og fællesanmeldelser, se kapitel 4.4.1.1 og

4.4.1 Den offentlige sektor

Behandlinger, som ikke omfatter personoplysninger af fortrolig eller følsom karakter, er undtaget fra anmeldelsespligten. I den sammenhæng skal det nævnes, at behandling af identifikationsoplysninger, f.eks. CPR-nummeret, selv om det betragtes som en fortrolig oplysning, ikke skal anmeldes til Datatilsynet. Nogle typer af behandlinger, som er nævnt i Justitsministeriets bekendtgørelse nr. 529 af 15. juni 2000 om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning, er undtaget fra anmeldelsespligten – f.eks. personaleadministrations- og undervisningssystemer.

En anmeldelse kan omfatte en eller flere databehandlinger, hvis formål er identiske eller logisk sammenhængende.

I en række tilfælde skal der ikke alene foretages anmeldelse, men tillige indhentes forudgående udtalelse fra Datatilsynet. Dette er tilfældet i følgende situationer:

- hvis behandlingen omfatter følsomme oplysninger. Det gælder f.eks. oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om

helbredsmæssige og seksuelle forhold samt strafbare forhold, væsentlige sociale problemer og andre rent private forhold[70]

- hvis behandlingen omfatter sammenstilling eller samkøring af oplysninger i kontroløjemed
- hvis behandlingen udelukkende finder sted med henblik på at føre retsinformationssystemer
- hvis behandlingen udelukkende finder sted i videnskabeligt eller statistisk øjemed

Det er ikke de enkelte registre eller IT-systemer, men derimod **behandlinger af personoplysninger**, der skal anmeldes. En anmeldelse skal udformes som en generel beskrivelse af myndighedens sagsgange vedrørende et bestemt sagsområde. Myndigheden behøver derfor alene én anmeldelse på et område, selv om der benyttes mere end ét IT-system.

Hvis myndigheden benytter systemer, hvor data behandles hos en ekstern leverandør, skal disse leverandører anføres som databehandlere på anmeldelsesblanketten.

4.4.1.1 Paraplyanmeldelser[71]

For at forenkle anmeldelsesproceduren har regionerne og Datatilsynet i fællesskab udarbejdet et antal såkaldte **paraplyanmeldelser**, der omfatter regionernes behandlinger på sundhedsområdet. En paraplyanmeldelse indeholder anmeldelse af flere databehandlinger.

Formålet med den forenklede procedure er at reducere antallet af anmeldelser på det regionale område samt at medvirke til, at den enkelte region kan bevare overblikket over regionens samlede aktiviteter.

Anmeldelse til Datatilsynet af behandling af personoplysninger, som en region er dataansvarlig for, sker centralt fra den pågældende region.

I den anledning har hver region udpeget en **kontaktperson**, som varetager opgaven med at koordinere og foretage de nødvendige anmeldelser og evt. ændringer i paraplyanmeldelserne til Datatilsynet.

Regionernes kontaktpersoner kan findes på Datatilsynets hjemmeside.

4.4.1.2 Fællesanmeldelser[72]

Fællesanmeldelser er anmeldelser til Datatilsynet af databehandlinger, der foretages på samme måde hos flere forskellige myndigheder, og anvendes især af kommunerne.

I en fællesanmeldelse udfylder den dataansvarlige kun et begrænset antal individuelle felter. De øvrige felter er i udfyldt i forvejen og beskriver den databehandling, som alle

[70] Persondataloven, § 45

[71] Se Datatilsynets hjemmeside, https://www.datatilsynet.dk/offentlig/forskning/forskning-i-regionerne/

[72] Se Datatilsynets hjemmeside, https://www.datatilsynet.dk/blanketter/offentlig-sektor/faellesanmeldelser/faellesanmeldelser-vejledning/

de tilsluttede myndigheder alle foretager som led i løsningen af de opgaver, der er beskrevet i fællesanmeldelsen.

KL og Datatilsynet har i samarbejde udformet en række "moderanmeldelser", der dækker en stor del af de databehandlinger, som de fleste kommuner foretager, og KL fungerer som koordinator i forhold til disse fællesanmeldelser.

Datatilsynet har desuden udformet fællesanmeldelserne "Videnskabelige og statistiske undersøgelser hos statslige myndigheder", "Videnskabelige og statistiske undersøgelser hos kommuner" samt "Forskningsbiobank(er) ved statslig myndighed".

Udfyldelse af en fællesanmeldelse skal ske elektronisk via Datatilsynets hjemmeside, som afgiver en udtalelse til den dataansvarlige myndighed om tiltrædelse til anmeldelsen og det offentliggøres i Datatilsynets fortegnelse over anmeldte behandlinger.

Ændringer i fællesanmeldelsernes faste del sker via KL, mens den dataansvarlige myndighed har pligt til at sørge for, at de individuelle oplysninger, f.eks. oplysning om ny databehandler, til stadighed holdes ajour over for Datatilsynet.

4.4.1.2 Anmeldelse af behandling i videnskabeligt eller statistisk øjemed

I regionerne er der udarbejdet to paraplyanmeldelser, der dels dækker den forskning på sundhedsområdet, der foregår i regionernes regi, dels de kliniske kvalitetsdatabaser, som regionen er dataansvarlig for.

Anmeldelsen "Sundhedsvidenskabelig forskning i Region X" dækker den løbende forskning i sygdomsforebyggelse, sygdomsbehandling og sundhedsfremme samt klinisk, epidemiologisk forskning inden for en række nærmere beskrevne områder. Anmeldelsen omfatter også større og længerevarende kliniske databaser og projekter. Omfattet af anmeldelsen er desuden biologisk materiale i biobanker, der er knyttet til konkrete forskningsprojekter og biobanker til fremtidig brug. Regionerne indsender én gang årligt en oversigt over igangværende forskningsdatabaser og -projekter til Datatilsynet.

Anmeldelsen "Kliniske kvalitetsdatabaser, der er godkendt af Sundhedsdatastyrelsen" dækker de kliniske kvalitetsdatabaser, der – med udgangspunkt i det enkelte patientforløb[73] (se kapitel 3.2.2.) – skal belyse og bidrage til forbedring af kvaliteten af sundhedsvæsenets indsats. Anmeldelsen omfatter kun kliniske kvalitetsdatabaser, der er godkendt af Sundhedsdatastyrelsen. Databaserne kan være regionale eller landsdækkende.

Regionernes anmeldelser findes på Datatilsynets hjemmeside.

[73] Jf. sundhedsloven, § 196

For kommuner og statslige myndigheder har Datatilsynet fra 2015 indført en ny og forenklet fremgangsmåde for anmeldelse af behandling personoplysninger, der udelukkende finder sted i videnskabeligt eller statistisk øjemed.

Ligesom for regionerne skal de statslige myndigheder og kommunerne kun foretage én samlet anmeldelse af de databehandlinger, som myndigheden foretager i videnskabeligt eller statistisk øjemed.

Inden behandlingen af personoplysninger i forbindelse med videnskabelige eller statistiske undersøgelser igangsættes, skal der derfor ikke ske anmeldelse direkte til Datatilsynet, men man skal henvende sig til den kontaktperson, som kommunen, regionen eller den statslige myndighed har udpeget.

4.4.1.4 Anmeldelser af ph.d.-projekter[74]

Der gennemføres en række ph.d.-projekter ved regionernes sygehusafdelinger. Projekterne involverer ofte afdelingens patienter, og den ph.d.-studerende vejledes af afdelingens overlæger.

Regionerne har i fællesskab udarbejdet retningslinjer for anmeldelse til Datatilsynet af "forsker-initieret sundhedsforskning i regionerne". Retningslinjerne kan findes på Danske Regioners hjemmeside.

4.4.1.5. Ændring af anmeldte behandlinger[75]

Hvis en myndighed vil ændre i de forhold, der er beskrevet i en anmeldelse til Datatilsynet, skal den anmelde dette til Datatilsynet. I regionerne skal ændringer i en anmeldelse ske via regionens kontaktperson.

Ændringer i fællesanmeldelsernes faste del sker som oftest via KL, mens den dataansvarlige myndighed har pligt til at sørge for, at de individuelle oplysninger, f.eks. oplysning om ny databehandler, til stadighed holdes ajour over for Datatilsynet.

Ændringer af behandlinger, som er omfattet af persondatalovens § 45, stk. 1 eller 2 – dvs. anmeldelser af den type behandlinger, der først må iværksættes efter, at Datatilsynet har afgivet udtalelse – skal tilsynet normalt udtale sig om, før ændringen iværksættes.

Ændringer af mindre væsentlig betydning kan anmeldes efterfølgende – senest 4 uger efter iværksættelsen[76].

4.4.2 Den private sektor

I den private del af sundhedssektoren skal der ligeledes foretages anmeldelse af behandling af fortrolige og følsomme oplysninger. Private aktører skal anmelde direkte til Datatilsynet, via Datatilsynets hjemmeside.

---

[74] Se Datatilsynets hjemmeside, http://www.datatilsynet.dk/offentlig/forskning/forskning-i-regionerne/

[75] Se Datatilsynets hjemmeside, https://www.datatilsynet.dk/blanketter/anmeld-aendring/

[76] Persondataloven, §46, stk. 1

Også i den private sektor skal der i en række tilfælde foretages anmeldelse samt indhentes forudgående tilladelse fra Datatilsynet. Dette er tilfældet, hvis behandlingen omfatter følsomme oplysninger[77].

Der er dog en undtagelse fra denne pligt, hvis personoplysningerne alene anvendes til brug for deres opgaver i relation til patientbehandling.

Private skal ikke anmelde databehandling, der sker i behandlingsøjemed

Af persondataloven78 fremgår det, at der ikke skal foretages anmeldelse, hvis:

- behandlingen foretages af læger, sygeplejersker, tandlæger, kliniske tandteknikere, apotekere, terapiassistenter, kiropraktorer og lignende personer med autorisation til at udøve virksomhed inden for sundheds- og sygeplejen, i det omfang oplysningerne alene anvendes til brug ved denne virksomhed og behandlingen af oplysningerne ikke sker for et privat sygehus
- behandlingen foretages til bedriftssundhedstjeneste

Som for den offentlige sektor er der desuden en undtagelsesbekendtgørelse for den private sektor

Af bekendtgørelsen fremgår, at bl.a. at der ikke er krav om anmeldelse til Datatilsynet, hvis behandling af personoplysninger sker i forbindelse med:

- kliniske forsøg med lægemidler omfattet af lov om lægemidler
- kliniske afprøvninger af medicinsk udstyr omfattet af lov om medicinsk udstyr,
- sundhedsvidenskabelige forskningsprojekter omfattet af lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter
- pligtmæssig sikkerhedsovervågning af lægemidler og medicinsk udstyr efter lov om lægemidler eller lov om medicinsk udstyr
- behandling af personoplysninger, som foretages af studerende under arbejdet med projekt- og specialeopgaver mv. som led i deres erhvervsakademi-, professionsbachelor-, bachelor- eller kandidatuddannelse eller uddannelse på tilsvarende niveau, når behandlingen sker med udtrykkeligt samtykke fra den registrerede

Dog skal non-interventionsforskning og indsamling og opbevaring af materiale til fremtidig forskningsbrug altid anmeldes.

4.4.4 Anmeldelse på Datatilsynets hjemmeside

Anmeldelse skal ske elektronisk via Datatilsynets hjemmeside

4.5 Overblik over dataflow

Den dataansvarlige har ansvaret for at vide, hvor og hvordan de oplysninger, de har ansvaret for, behandles.

[77] Persondataloven, §§7-8

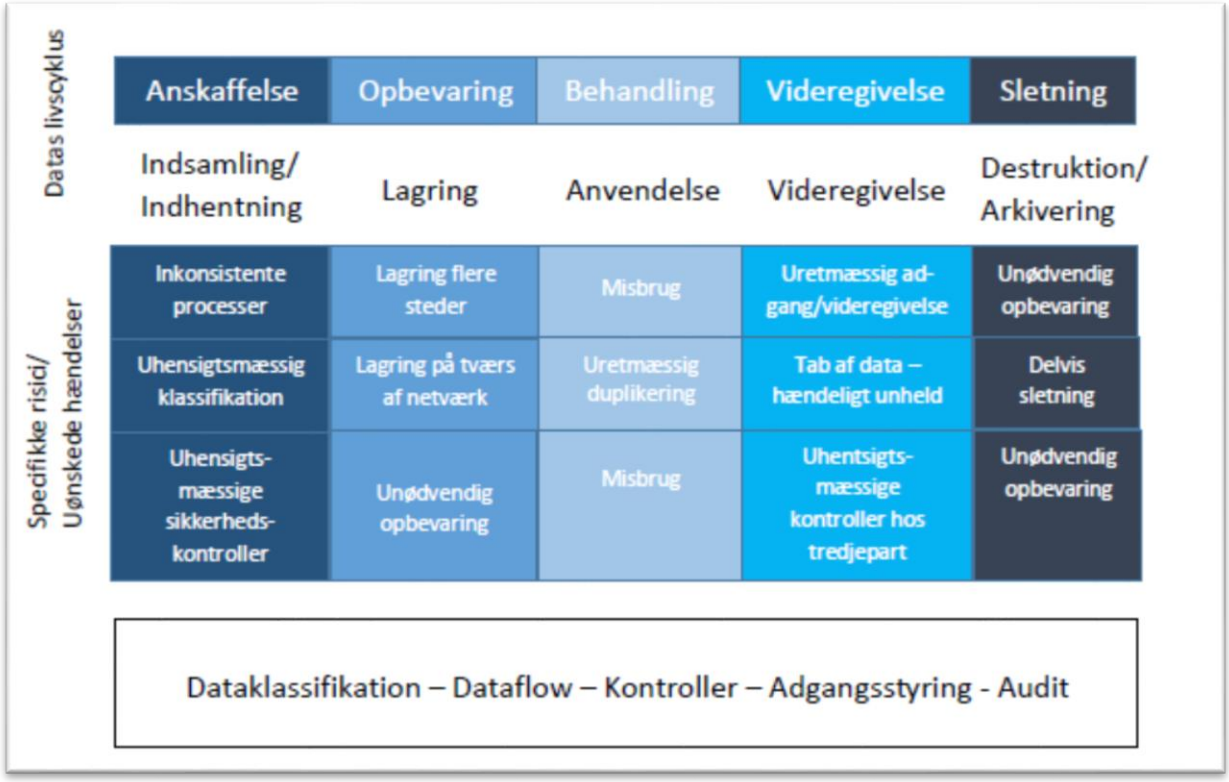
[78] Persondataloven, § 49, stk. 1, pkt. 8-9

For at skaffe sig dette overblik, kan der foretages en kortlægning af datas livscyklus og vandring mellem den dataansvarlige, databehandlere og eventuelle tredjeparter i form af en dataflowanalyse. Dataflowanalysen kan afdække hvilke personoplysninger, som kommer ind i og forlader organisationen, hvordan, hvorfor, hvilken behandling der finder sted, og hvem der har adgang til personoplysningerne.

En dataflowanalyse kan indeholde følgende punkter:

1. Hvilke personoplysninger vil blive behandlet?
2. Hvilke teknologier anvendes?
3. Hvilke kilder er der til personoplysningerne?
4. Hvordan foregår indsamlingen af personoplysninger?
5. Hvilket formål man har med at behandle personoplysningerne?
6. Sikres det, at der ikke indsamles flere oplysninger end formålet tilsiger?
7. Sikres det, at oplysninger ikke anvendes til andre formål?
8. Sletningsregler for evt. midlertidige kopier af datasættet
9. Kortlægge hvilken behandling af oplysninger, der finder sted
10. Bestemme hvem der har adgang til personoplysninger
11. Bestemme hvem der er ansvarlig for oplysningernes sikkerhed
12. Hvordan organiseres personoplysningerne?
13. Videregives oplysninger til andre?
14. Slettes oplysninger, når behandlingsformålet ophører?

Beskrivelsen kan omfatte både indsamling, opbevaring behandling, videregivelse og sletning, f.eks. i form af et dataflowdiagram, jf. nedenstående oversigt, som også beskriver nogle af de risici, som man bør være opmærksom på i de forskellige faser samt nederst nogle af de værktøjer, der med fordel kan anvendes til at skabe sig det nødvendige overblik over dataflowet.



Figur 4.1 Dataflowanalyse

5. Deling af oplysninger på tværs af sektorer

Med udgangspunkt i de lovgivningsmæssige rammer, som blev beskrevet i kapitel 3, beskrives i dette kapitel, under hvilke betingelser, der kan ske deling af oplysninger på tværs af sundhedssektoren, dvs. f.eks. mellem forskellige forvaltninger i kommunerne, sygehuse og praktiserende læger samt forslag til, hvordan man kan aftale og dokumentere datadeling, så det er i overensstemmelse med lovkravene.

Deling af oplysninger bliver ofte brugt til at udtrykke, at der er behov for, at oplysningerne kan bruges af forskellige sundhedspersoner i deres behandling af patienten. I lovgivningsmæssig forstand er der tale om **videregivelse** eller **indhentning** af oplysninger, jf. kapitel 3.

Sundhedsvæsenet udvikler sig hele tiden og nye behandlingsformer og teknologi betyder, at mange undersøgelser og behandlinger kan foretages uden for sygehusene i samarbejde med eksempelvis praktiserende læger eller personale i kommunerne.

Inden for sygehusområdet sker der en specialisering af sygehusene, som betyder, at patienter i langt højere grad end tidligere, behandles på flere sygehuse i løbet af et behandlingsforløb. F.eks. kan forundersøgelse foregå på et lokalt sygehus, mens operationen foregår på en specialafdeling, og at man derefter tilbydes genoptræning på det lokale sygehus eller et andet sygehus, der udbyder denne ydelse.

Flere regioner har indgået aftaler med private sygehuse og klinikker om udførelse af bestemte sundhedsydelser, som tidligere er foregået i offentligt regi og mange kommuner samarbejder med private leverandører af sundhedsydelser, f.eks. til praktisk hjælp og hjælpemidler. Også her er der behov for at kunne dele patientoplysninger.

Endelig er der på nationalt plan etableret flere løsninger, som stiller oplysninger til rådighed for sundhedsvæsenets parter. Sundhedsdatastyrelsen driver det Fælles Medicinkort og regionerne udstiller via sundhed.dk Sundhedsjournalen.

5.1 Hvordan deles oplysninger?

Deling af oplysninger mellem sundhedsvæsenets parter kan foregå på flere forskellige måder.

Den hyppigst anvendte kommunikationsform er nok MedCom meddelelser, der anvendes på en række områder til at informere andre parter i sundhedsvæsenet. Som det fremgår af navnet, er kommunikationen meddelelsesbaseret, hvilket vil sige, at en afsender sender en besked/meddelelse til en modtager, f.eks. et udskrivningsbrev til egen læge, en rekvisition til et laboratorie eller en advis til kommunen om, at en borger med tilknytning til ældreplejen, er blevet indlagt.

Herudover kan oplysningerne - når der er hjemmel hertil - deles ved, at de placeres i en database, som flere myndigheder, sundhedspersoner mv. har adgang til, som det f.eks. sker i det Fælles Medicinkort. Her kan en sundhedsperson, som har de fornødne brugerrettigheder og en aktuel behandlingsrelation, få adgang til oplysningerne, når det er nødvendigt.

Herudover er det muligt at kommunikere mellem parterne med anvendelse af sikker e-mail.

5.2 Betingelser for deling af oplysninger på sundhedsområdet

Den dataansvarlige skal sikre sig, at der er hjemmel i lovgivningen til at indsamle og videregive oplysningerne til andre parter i sundhedsvæsenet. I dette kapitel forudsættes, at oplysninger er lovligt indhentet, og kapitlet beskriver derfor alene betingelser for videregivelse og elektronisk indhentning.

Det er ikke alene sundhedspersonens organisatoriske placering, men også om vedkommende har en aktuel behandlingsrelation til patienten inden for egen behandlingsenhed, der er afgørende for adgangen til oplysningerne, og om oplysninger kan deles på tværs af sundhedsvæsenet.

Patientoplysninger må, som beskrevet i kapitel 3, videregives eller indhentes elektronisk uden patientens samtykke, hvis:

- Det sker i forbindelse med et aktuelt behandlingsforløb
- Den, oplysninger videregives til eller som elektronisk indhenter oplysninger, skal være berettiget hertil og have en aktuel behandlingsrelation til patienten
- De oplysninger, der videregives eller indhentes, er nødvendige for, at sundhedspersonen kan udføre sin opgave i relation til den aktuelle patientbehandling
- Patienten har ikke frabedt sig videregivelse eller indhentning af de pågældende oplysninger. Patienten skal være informeret om, hvilke personer eller persongrupper, man vil dele oplysninger med.

I tværsektorielle projekter, hvor der skal ske deling af oplysninger, er det væsentligt, at der inden indsamling af oplysninger igangsættes, tages stilling til, hvem der dataansvarlig for oplysninger og dermed sætter rammerne for anvendelsen af oplysninger med udgangspunkt i sundhedslovens bestemmelser.

Det anbefales, at den eller de dataansvarlige i forbindelse med, at der indgås aftaler om deling af oplysninger mellem parter i sundhedsvæsenet, f.eks. i forbindelse med etablering af en telemedicinsk løsning, hvor oplysninger skal deles mellem f.eks. personale i kommunen og på sygehuset, gennemgår sin systemportefølje:

- fra hvilke systemer(databehandlinger) stammer de oplysninger, man ønsker at dele?
- er delingen omfattet af lovhjemmel i sundhedsloven eller særlovgivning?
- er formålet med delingen omfattet af formålet for databehandlingen, som det fremgår af den eksisterende anmeldelse til Datatilsynet?
- arbejdes der med flere lovgivninger på området? Hvis oplysninger om patientens helbredstilstand skal bruges til andre formål end sundhedsydelser i kommunerne, kan det være serviceloven eller forvaltningsloven, der sammen med persondataloven sætter rammerne for dataanvendelsen.
- er der hjemmel i lovgivningen til deling af oplysningerne? Hvis ikke der er hjemmel i særlovgivningen, skal hjemlen findes i persondataloven. Hjemlen kan være et samtykke fra den registrerede.

Hvis formålet ikke er omfattet af den eksisterende anmeldelse, skal der evt. ske anmeldelse af en ændring til Datatilsynet (se kap. 4.4). Hvis der er tale om et helt nyt formål, skal der sandsynligvis laves en ny anmeldelse og man må kun dele oplysninger, der er registreret efter Datatilsynets godkendelse. Derfor er det vigtigt, at man tidligt i forløbet vurderer, om der er behov for at ændre i sine anmeldelser til Datatilsynet, så det ikke bliver et forsinkende led.

Ligeledes skal der tages specifikt stilling til, hvilke informationer, de forskellige faggrupper skal og må have adgang til.

For eksempel skal det personale i kommunerne, som skal modtage en patient efter et sygehusophold og sikre, at de rigtige ydelser stilles til rådighed, kun have adgang til de oplysninger fra den elektroniske patientjournal, der er nødvendige for udførelsen af deres opgaver.

For de i sundhedslovens § 42a, stk. 2, nævnte sundhedspersoner[79] er der endvidere krav til, at adgangen for den pågældende sundhedsperson teknisk skal være begrænset til de patienter, der er i behandling på samme behandlingsenhed, som den pågældende sundhedsperson er tilknyttet.

[79] Sundhedspersoner, der *ikke* er læger, tandlæger, jordemødre, sygeplejersker, sundhedsplejersker, social- og sundhedsassistenter, radiografer, ambulancebehandlere med særlig kompetence eller kiropraktorer

For at dokumentere, at datadeling mellem forskellige parter på sundhedsområder lever op til den hjemmel i lovgivningen, som den vedrører, anbefales det, at der udarbejdes et aftalegrundlag, som beskriver de enkelte parters ansvar og forudsætningerne for aftalen:

- Dataansvarlig(e)
- Databehandlere
- Modtagere
- Formål med deling af oplysninger
- Oplysninger, omfattet af aftalen
- Relevant lovgivning
- Hjemmel til indsamling
- Faggruppers adgang til forskellige typer af oplysninger
- Dataintegritet
- Overholdelse af standard vedr. informationssikkerhed (ISO27001, se kapitel 12)

I nogle tilfælde vil det ikke være nødvendigt at udarbejde en konkret aftale. For eksempel indgår deling af oplysninger mellem sygehuse, der deltager i den aktuelle patientbehandling eller udsendelse af udskrivningsbrev (epikrise) til egen læge efter sygehusophold, direkte i sundhedsloven eller bekendtgørelser i forhold til sundhedsloven (se kap. 3).

Hvis man vil indgå en aftale om deling af oplysninger med private aktører – private leverandører eller sundhedspersoner i praksissektoren – skal det aftales, hvordan man opnår det nødvendige informationssikkerhedsniveau i behandlingen af patientoplysningerne hos den private aktør og i kommunikationen med denne, og der skal gøres de samme overvejelser, undersøgelser og tiltag, som hvis der alene er tale om offentlige aktører.

Den dataansvarlige skal altid have styr på, hvor de oplysninger, vedkommende har ansvaret for, anvendes hen og hvem, der har adgang til oplysninger.

For at sikre, at de oplysninger, der deles mellem parterne kan ses korrekt af alle parter, skal man i forbindelse med aftaler om datadeling også sikre sig, at der ikke sker en forvanskning af oplysninger, hvis de f.eks. bliver vist som en integreret del af et it-system. Det gælder både i forhold til at sikre sig, at oplysninger er komplette, at de ikke er blevet ændret og at den kontekst, de indgår i, er kendt, hvor det er relevant. F.eks. har man i FMK-projektet gennem certificering sikret sig, at medicindata, der udveksles mellem det centrale FMK og de lokale journalsystemer, vises korrekt i sygehusenes medicinsystemer og i lægepraksissystemerne.

Jo større udbredelse elektronisk deling af oplysninger får og jo mere afhængig, sundhedspersoner bliver af de elektroniske løsninger, jo vigtigere bliver det at sikre dataintegriteten, så forkerte eller forældede oplysninger ikke fører til fejlbehandling.

I den sammenhæng bør man ligeledes se på de indholdsmæssige standarder, der anvendes hos de parter, der indgår i datadelingen, og vurdere, om der er behov for at mappe oplysninger, så der ikke sker misforståelser mellem parterne

5.3 Landsdækkende databaser

På enkelte områder er der etableret lovhjemmel til at etablere landsdækkende databaser, hvor der er en dataansvarlig, som sikrer, at data anvendes i henhold til formål og lovhjemmel.

Eksempler på sådanne landsdækkende databaser er det Fælles Medicinkort[80], det Danske Vaccinationsregister[81] og det Nationale Patientindeks[82].

[80] Sundhedsloven, § 157

[81] Sundhedsloven, § 157b

[82] Sundhedsloven, §193b

6. Adgang til borgerens oplysninger

I dag registreres der ikke kun helbredsoplysninger om borgerne i forbindelse med behandling i sundhedsvæsenet, men mange borgere begynder at opsamle oplysninger om deres helbred i apps på deres mobiltelefon, i deres ur, i Microsoft HealthVault eller andre privat udbudte løsninger.

Der skal derfor skelnes mellem patientoplysninger, som en sundhedsperson "bestiller" eller beder om, at borgeren registrer med henblik på en konkret udredning, behandling e.l. på den ene side og oplysninger om velbefindende, som borgeren typisk selv genererer og lagrer, på den anden side.

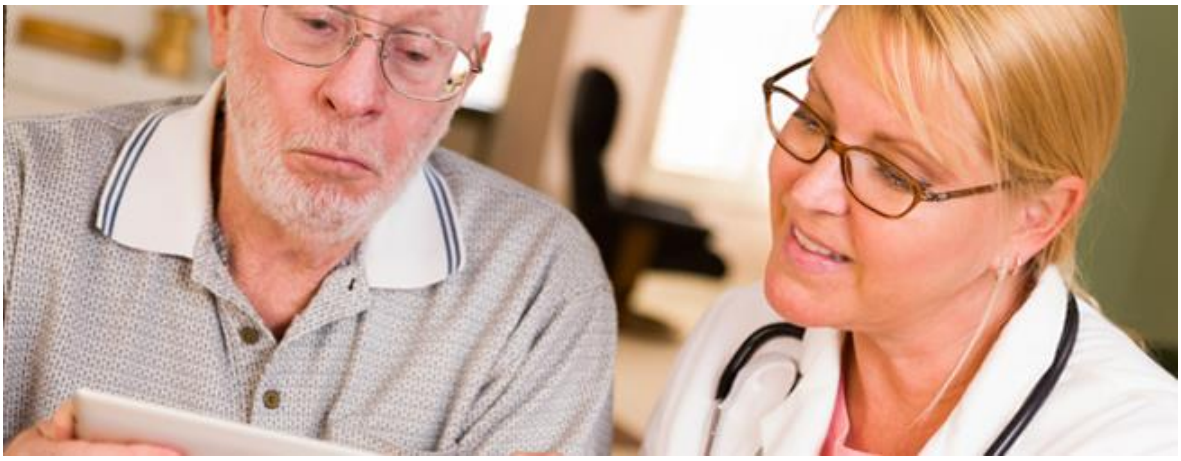
Hvor oplysninger, som en sundhedsperson beder borgeren om at registrere til brug for behandling e.l., er omfattet af persondataloven og sundhedsloven, er de data, borgeren på eget initiativ opsamler og lagrer, ikke reguleret i sundhedsloven. Persondataloven finder heller ikke anvendelse for behandlinger, som en fysisk person foretager med henblik på udøvelse af aktiviteter af rent privat karakter[83], men hvad der er omfattet af bestemmelsen beror på en konkret vurdering, og der kan derfor være situationer, hvor persondataloven finder anvendelse, hvis borgeren opsamler oplysninger på eget initiativ.

Sundhedspersoner er derfor som udgangspunkt ikke forpligtet til at forholde sig til de oplysninger, som en borger selv har indsamlet, men i det omfang, at oplysningerne kan bidrage til udredningen af patientens tilstand, kan sundhedspersonen anvende disse oplysninger, hvis de forekommer at have tilstrækkelig relevans og kvalitet.

Borgerens egne oplysninger er ikke patientoplysninger. Det bliver de, hvis en sundhedsperson vælger at inddrage dem i behandlingen af patienten og journalfører oplysningerne i et sundheds-it system, f.eks. en elektronisk omsorgsjournal, patientjournal eller et lægepraksissystem. Hvis oplysninger overføres eller registreres i et

[83] Persondataloven, § 2, stk. 3

sundheds-it system, gælder de almindelige regler i sundhedsloven, persondataloven og retssikkerhedsloven m.v.



7. Borgerens adgang til oplysninger

Borgerne – og deres pårørende – har i større omfang end tidligere mulighed for at få adgang til deres egne sundhedsoplysninger. Ud over adgang til akt- og registerindsigt har borgerne også mulighed for elektronisk at få adgang til en række oplysninger om deres behandling på sundhed.dk og her kan de også for nogle it-løsninger se, hvem der har haft adgang til deres oplysninger.

7.1 Ret til indsigt og aktindsigt

Patienters adgang til aktindsigt i deres patientjournal er beskrevet i sundhedslovens kapitel 8. Sundhedslovens regler gælder for aktindsigt i regionernes patientjournaler, kommunernes omsorgsjournaler og journaler hos praktiserende læger mv. Alle autoriserede sundhedspersoners optegnelser er omfattet af kravet.

Herudover gælder generelt persondatalovens indsigtsret[84].

En patient, der er blevet undersøgt eller behandlet på et sygehus eller et andet behandlingssted har krav på at få aktindsigt i sin patientjournal og, hvis det ønskes, at få udleveret en kopi.

Der er ingen formkrav til patientens anmodning om aktindsigt, men afdelingen skal bede om legitimation, medmindre patienten eller den pårørende (forældre eller værge) er kendt af personalet.

Patienten har krav på aktindsigt i alle oplysninger indeholdt i den patientjournal, som sygehuset, den praktiserende læge eller andre sundhedspersoner er i besiddelse af, herunder oplysninger fra andre afdelinger eller sygehuse.

[84] Persondataloven, §31

Anmodning om aktindsigt skal efterkommes inden for 7 arbejdsdage og hvis dette ikke kan lade sig gøre, skal patienten informeres om årsagen hertil og hvornår anmodningen forventes at blive imødekommet.

For oplysninger i patientjournaler, der er journalført før 1. januar 2010 kan retten til aktindsigt begrænses, hvis der er afgørende hensyn til patienten selv eller andre private interesser, som man skal tage. For optegnelser, der er journalført efter denne dato, er der ikke denne mulighed for at begrænse aktindsigten.

Alle, der er fyldt 15 år, har ret til aktindsigt i egen journal.

På det kommunale område gælder, hvor det ikke er sundhedslovens bestemmelser, der er gældende, persondatalovens og forvaltningslovens regler om den registreredes ret til indsigt.

Borgeren har ret til indsigt i de oplysninger, der er registreret om vedkommende[85]. Anmodning om indsigt skal rettes til den dataansvarlige, som er forpligtet til at svare på, om der behandles oplysninger om den pågældende person og i givet fald give meddelelse om, hvilke oplysninger, der behandles, formålet med behandlingen, kategorier af modtagere af oplysningerne samt tilgængelig information om, hvorfra oplysningerne stammer.

Den dataansvarlige skal snarest besvare begæringer om indsigt. Er begæringen ikke besvaret inden 4 uger efter modtagelse, skal den dataansvarlige underrette den pågældende om grunden hertil, samt om, hvornår afgørelsen kan forventes at foreligge[86].

Adgangen til indsigt efter persondataloven gælder ikke, hvis oplysningerne udelukkende behandles i videnskabeligt øjemed[87], eller hvor oplysningerne kun opbevares i form af personoplysninger i det tidsrum, som kræves for at udarbejde statistikker. Retten til indsigt omfatter som udgangspunkt heller ikke oplysninger i sikkerhedslogs (systemmæssig facilitet som kræves efter sikkerhedsbekendtgørelsen ved visse behandlinger af personoplysninger).

7.2 Adgang til egne sundhedsoplysninger

Nogle, men ikke alle patientoplysninger kan tilgås af borgerne selv, f.eks. i sundhedsjournalen og det Fælles Medicinkort på sundhed.dk.

[85] Persondataloven, §31, stk. 1

[86] Persondataloven, §31, stk. 2

[87] Persondataloven, § 32, stk. 4

Ved anvendelse af NemID kan borgerne få adgang til oplysninger, der er registreret om dem, f.eks. epikriser, notater, laboratorieresultater og medicinoplysninger.

I nogle kommuner kan borgerne få adgang til egne oplysninger i den elektroniske omsorgsjournal.

7.3 Adgang til logoplysninger

I dag kan borgerne via sundhed.dk tilgå MinLog, hvor der for f.eks. FMK og sundhedsjournalen fremgår, hvem der har foretaget opslag på patientoplysninger. Det er indtil videre kun opslag på sundhed.dk, som kan ses i MinLog.

Sundhedslovens § 42c giver mulighed for, at ministeren kan fastsætte nærmere regler om borgernes adgang til elektronisk at se, hvem der har foretaget opslag på deres patientoplysninger.

I bemærkningerne til lovforslaget står, der, at denne bemyndigelse vil blive udnyttet, når det systemteknisk er muligt at generere de relevante oplysninger uden væsentlige administrative byrder.

Der er ikke på nuværende tidspunkt taget stilling til, hvornår alle eksisterende it-systemer på sundhedsområder skal kunne levere logoplysninger, men ved udvikling eller anskaffelse af nye it-løsninger bør man indtænke borgerens adgang til logoplysninger.

Selv om borgeren via f.eks. MinLog kan se, hvem der har haft adgang til deres oplysninger, er det stadig den dataansvarlige myndighed, der er forpligtet til at følge op på loggen gennem periodiske stikprøvekontroller eller hvis der er mistanke om et sikkerhedsbrud[88].

MinLog skal bidrage til at skabe åbenhed om dataanvendelsen i sundhedsvæsenet og give borgeren en tryghed for, at deres oplysninger kun anvendes til de godkendte formål.

Af MinLog kan borgeren se, hvem der har tilgået hvilke oplysninger i de forskellige systemer, der er tilknyttet, f.eks. det fælles medicinkort og sundhedsjournalen. Det er ikke i alle systemer, at borgeren kan se navnet på den konkrete person, der har foretaget opslaget, idet der i nogle systemer kun angives en rolle og en organisation (apotek, sygehusafdeling e.l.). I disse tilfælde kan man finde frem til den konkrete bruger i det bagvedliggende system, hvor det er registreret. Dette sker for at afveje hensynet til åbenhed over for borgeren og hensynet til sundhedspersoner, der evt. kan blive forfulgt af personer, der mener, at de er blevet forkert behandlet eller lignende.

[88] Sikkerhedsbekendtgørelsen, §19, stk. 1

7.4 Adgang for pårørende, værger m.v.

7.4.1 Forældremyndighed eller værgemål

Som forældre med forældremyndighed over en person under 18 år kan man få aktindsigt i barnets eller den unges journal. Forældremyndighedsindehaveren har krav på aktindsigt i den fulde journal, medmindre hensyn til barnet eller den unge overstiger forældrenes interesse i at blive oplyst om en given behandling[89].

Selv om man ikke er indehaver af forældremyndigheden, har man som forældre lov til at blive orienteret om barnets helbred, jf. forældreansvarslovens §23. Heraf følger, at oplysninger, der er relevante for pasning af barnet kan videregives til den af forældrene, der ikke har forældremyndigheden.

Hvis en borger ikke kan tage vare på sine egne interesser, indtræder den legale repræsentant i patientens rettigheder efter loven. Den legale repræsentant kan være indehaveren af forældremyndigheden, nærmeste pårørende eller en værge[90].

Adgang til oplysninger for den legale repræsentant er begrænset til forhold, der er relevante for at varetage borgerens interesser og behov i den konkrete situation. I det omfang, det er relevant, kan en værge få adgang til journaloplysninger.

7.4.2 Samtykke og fuldmagt

I forbindelse med behandling på et sygehus udfyldes der som oftest en samtykkeerklæring, hvor man som borger kan give samtykke til, at ens pårørende bliver orienteret om behandlingen. Hvis den pårørende derimod skal have aktindsigt i journal mv., kræves der en fuldmagt fra den person, det vedrører.

Der videregives oplysninger til en tredjepart, f.eks. en pårørende eller en anden, der repræsenterer patienten, forudsat, at borgeren har givet fuldmagt til det91. Der er begrænsninger knyttet til fuldmagter til pårørende, der således ikke automatisk kan få fuld aktindsigt.

For så vidt angår demente er det en konkret vurdering, om der er tale om en varigt inhabil patient. Hvis den demente ikke er varigt inhabil, gælder der samme regler for denne som for habile patienter. Det anbefales dog, at underskrivelse af en eventuel fuldmagt overværes og skriftligt bevidnes af uafhængige vidner, for at undgå eventuel tvivl om, hvorvidt den demente har underskrevet fuldmagten frivilligt.

---

[89] Sundhedsloven, § 17

[90] Sundhedsloven, § 18

[91] Sundhedsloven, kapitel 8

Hvis den demente må anses for varigt inhabil (og dermed ikke selv kan varetage sine interesser), fremgår det af sundhedsloven92, at den eller de personer, som efter lovgivningen er bemyndiget hertil, indtræder i patientens rettigheder i det omfang, det er nødvendigt for at varetage patientens interesser i den pågældende situation. For en patient, der varigt mangler evnen til at give informeret samtykke, kan de nærmeste pårørende give informeret samtykke til behandling. I de tilfælde, hvor patienten er under værgemål, der omfatter personlige forhold, herunder helbredsforhold, kan informeret samtykke dog gives af værgen93.

Fuldmagten skal være skriftlig, dateret og underskrevet af patienten. Digitaliseringsstyrelsen har udarbejdet en elektronisk fuldmagtsløsning, som er taget i drift i forhold til sundhedsjournalen. Der arbejdes på at udbrede anvendelsen af fuldmagtsløsningen i sundhedsvæsenet, f.eks. i forhold til FMK.

Myndigheder og forsikringsselskaber kan få videregivet helbredsoplysninger om patienten, hvis patienten har givet samtykke hertil i forbindelse med forsikringsansøgningen. Ved digitale ansøgninger kan man som sundhedsperson sikre sig dokumentation for den digitale underskrifts rigtighed ved at anmode om en kopi af PID[94].

Hvis journalen indeholder oplysninger, der ikke er relevante for forsikringsselskabet, skal disse udelades. Sundhedsvæsenets personale, herunder patienternes egen læge har et ansvar for at sikre, at kun relevante oplysninger videregives.

Forsikringsselskaber må ikke indhente oplysninger om arveanlæg og risiko for at udvikle eller pådrage sig sygdomme, hvis det ikke handler om den aktuelle helbredstilstand[95].

7.4.3 Dødsfald

Nærmeste pårørende har ret til efter anmodning at få oplysninger om sygdomsforløb, dødsårsag og dødsmåde, såfremt det ikke strider mod den afdødes udtrykkelige ønske, og hensynet til den døde eller andre private interesser ikke taler afgørende imod[96]. Andre oplysninger end de nævnte har den pårørende ikke ret til at se.

Ved nærmeste pårørende forstås i udgangspunktet ægtefælle eller samlevende og pårørende i lige linje: Hvis disse ikke lever eller borgeren har angivet ønske herom, kan nærmeste pårørende være en anden person, der stod afdøde nær i forløbet op til dødsfaldet, eller en person, som afdøde selv har oplyst som nærmeste pårørende.

---

[92] Sundhedsloven, §14

[93] Sundhedsloven, § 18

[94] Person-ID i den digitale signatur

[95] Lov om forsikringsaftaler, §3a

https://www.retsinformation.dk/forms/r0710.aspx?id=143090

[96] Sundhedsloven, §45

Adgang til aktindsigt ved patientens død kræver et samtykke fra den afdøde. Som udgangspunkt er dette reguleret af sundhedslovens §43, stk. 2. Dette samtykke bortfalder som udgangspunkt efter 1 år, men i en afgørelse fra Patientombuddet i 2015 har klageren fået ret i, at samtykket burde gælde, også efter en længere periode.

Pårørende kan efter en konkret vurdering og med anvendelse af værdispringsreglen[97] få oplysninger videregivet i yderligere omfang uden den afdødes samtykke, men et sådant kan indgå i vurdering efter værdispringsreglen.

[97] Sundhedsloven, §2, stk. 2

8. Anvendelse af personoplysninger til videnskabeligt eller statistisk formål

De oplysninger, der indsamles og registreres i forbindelse med patientbehandlingen, anvendes i stort omfang til sekundære formål, herunder til epidemiologisk forskning, overvågning, forskning i nye behandlingsmetoder, statistik m.m. Både sundhedsloven og persondataloven indeholder krav til, hvordan personoplysninger skal behandles og beskyttes i denne sammenhæng, jf. denne vejlednings kapitel 4.

8.1 Sundhedsvidenskabelig forskning på mennesker eller biologisk materiale

Alle sundhedsvidenskabelige forskningsprojekter, der involverer undersøgelse af mennesker eller menneskeligt biologisk materiale, skal være godkendt i en videnskabsetisk komité, inden det må igangsættes.

Anmeldelse af et forskningsprojekt sker til en af de regionale videnskabsetiske komiteer ved at anvende komitesystemets anmeldelsesportal eller ved komplekse sager til den nationale videnskabsetiske komité. Hvis der er tale om kliniske lægemiddelforsøg på den fælles anmeldelsesportal for kliniske lægemiddelforsøg.

I forhold til de helbredsoplysninger o.l., der indsamles i forbindelse med et projekt, er disse underlagt persondataloven og skal anmeldes til Datatilsynet som beskrevet i kapitel 5, dog ikke hvis der arbejdes med anonymiserede oplysninger, jf. kapitel 8.8.

De indsamlede oplysninger må kun anvendes til det konkrete forskningsprojekt og til det forskningsformål, som er angivet og det er kun den dataansvarlige og dem, der arbejder på vegne af den dataansvarlige, som må have adgang til personoplysninger.

Videregivelse til tredjemand må kun ske til statistiske eller videnskabelige formål og det kræver Datatilsynets godkendelse, inden oplysninger må videregives.

> Oplysninger, der indsamles til brug ved videnskabelige eller statiske undersøgelser, må ikke videregives eller anvendes til brug for konkret patientbehandling.

Hvis der kommer væsentlige oplysninger om forsøgspersonens helbredsstilstand frem under forskningsprojektet, skal forsøgspersonen informeres herom, med mindre de utvetydigt har frabedt sig dette[98].

Hvis der under et sundhedsvidenskabelige forskningsprojekter med omfattende kortlægning af den menneskelige arvemasse fremkommer tilfældighedsfund vedrørende forsøgsdeltageren, bør der ske tilbagemelding om alvorlig genetisk betinget sygdom, hvis

- der er en rimelig grad af sandsynlighed for, at en genetisk disposition er til stede,
- der foreligger en sikker dokumenteret sammenhæng mellem den genetiske disposition og sygdomsudviklingen,
- de tests, som benyttes for at fastslå den genetiske disposition, er sikre,
- sygdommen i væsentlig grad kan forebygges eller behandles, og
- sammenhængen har en væsentlig betydning for forsøgspersonen[99].

Hvis man indsamler oplysninger fra patientjournalen hos de patienter, der indgår i projektet, skal de orienteres herom i deltagerinformationen, ligesom det skal oplyses, hvis andre, fx sponsor og monitorer og danske og udenlandske kontrolmyndigheder for adgang til relevante oplysninger heri[100].

[98] Bekendtgørelse nr. 1149 af 30. september 2013 om information og samtykke til deltagelse i sundhedsvidenskabelige forskningsprojekter samt anmeldelse af og tilsyn med sundhedsvidenskabelige forskningsprojekter, § 15

https://www.retsinformation.dk/forms/R0710.aspx?id=158259

[99] Retningslinjer for komitésystemets behandling af sundhedsvidenskabelige forskningsprojekter med omfattende kortlægning af individets arvemasse, version 5, afsnit 3.1.

http://www.dnvk.dk/~/media/Files/cvk/forskere/Hvordan%20soeger%20jeg/Retningslinjer%20genom%20Version%205%20DOR10040S.ashx

[100] Komiteloven, §§ 3-6

Anvender man en ekstern databehandler, skal der indgås en databehandleraftale, jf. kapitel 5.

> Sundhedspersoner må ikke elektronisk indhente oplysninger til brug for forskning eller statistik fra elektroniske patientjournaler, sundhedsjournalen på sundhed.dk, Det Fælles Medicinkort e.l.

Når projektet er afsluttet, skal oplysningerne slettes eller anonymiseres på en sådan måde, at de ikke kan genskabes. Alternativt kan oplysninger overflyttes til Rigsarkivet efter arkivlovens regler[101].

Offentliggørelse af resultater fra projektet må udelukkende ske i anonymiseret form. Det må derfor ikke være muligt at identificere enkeltpersoner (se nedenfor om diskretionering).

Der gælder særlige krav ved overførsel af oplysninger til tredjelande eller ved anvendelse af databehandler i et tredjeland. Dette er behandlet i kapitel 9.

8.2 Videnskabelige og statistiske undersøgelser på basis af patientjournaler

Videnskabelige eller statistiske undersøgelser, der baserer sig på oplysninger fra patientjournaler skal enten være godkendt af en videnskabsetisk komité eller patienterne skal have givet samtykke til, at deres data videregives til forskningsprojektet. Hvis det ikke er muligt eller hensigtsmæssigt at indhente patienternes samtykke, skal der indhentes en godkendelse fra Sundhedsstyrelsen.

Herefter kan man få videregivet oplysninger fra patientjournaler, typisk ved at kontakte den eller de afdelinger, der er relevante i forhold til projektets formål. I nogle regioner er der etableret forskningsenheder, som hjælper med at indsamle information.

Hvis der er tale om større, landsdækkende projekter kan Forskerservice hos Sundhedsdatastyrelsen på baggrund af en godkendelse udlevere personnumre samt sygehus- og afdelingsoplysninger til forskerne, så de kan identificere de journaler, der er relevante at indhente oplysninger fra i forhold til projektets formål.

8.3 Registerforskning

I Danmark er der indsamlet mange oplysninger om patienter og deres behandling, som findes i en række statslige registre, som for nogens vedkommende har eksisteret i mange år. Cancerregisteret blev oprettet allerede i 1943 og Landspatientregisteret har eksisteret siden 1976. Det betyder, at der er et helt unikt materiale til rådighed for forskning på sundhedsområdet, som betyder, at man ofte kan anvende allerede

[101] Offentlighedsloven, § 21

eksisterende sundhedsdata i sin forskning fremfor at skulle starte med at indsamle oplysninger i en 5- eller 10-årig periode.

Registerforskning er forskningsaktiviteter, der helt eller delvist baseres på eksisterende sundhedsdataregistre og ofte indgår der oplysninger fra flere registre i sådanne studier.

Forskerservice ved Sundhedsdatastyrelsen har til formål at understøtte registerforskningen på sundhedsområdet og stiller data til rådighed til forskningsprojekter fra de nationale sundhedsregistre, som Sundhedsdatastyrelsen er dataansvarlig for.

Videregivelse af data fra sundhedsregistrene skal have hjemmel i persondataloven.

Som udgangspunkt kan forskerne få adgang til sundhedsregistrene via Forskermaskinen, hvor data i pseudonymiseret form stilles til rådighed. Databehandlingen foregår på Forskermaskinen, hvor hvert projekt oprettes med sin egen projektdatabase. Sundhedsdatastyrelsen er dataansvarlig for Forskermaskinen og de enkelte forskere er dataanvendere. De enkelte projektmapper, hvor forskerne lægger deres undersøgelsesresultater, er de selv dataansvarlige for og det er en forudsætning for adgang til Forskermaskinen, at deres projekt er godkendt af Datatilsynet.

Data fra de nationale sundhedsregistre kan herudover, hvor det er nødvendigt, stilles til rådighed som et skræddersyet udtræk, der sendes til forskerens arbejdsplads, og som enten kan være individdata eller aggregerede opgørelser. Der udleveres kun CPR-numre, hvis der er eksplicit behov herfor[102].

En anden mulighed er, at data sendes til Danmarks Statistik, hvis forskeren har en population på et projekt her og har behov for at få disse data beriget med data fra et eller flere af de nationale sundhedsregistre.

8.5 Biobanker

En biobank er en struktureret samling af menneskeligt biologisk materiale, der er tilgængeligt efter bestemte kriterier, og hvor oplysninger, der er bundet i det biologiske materiale, kan henføres til enkeltpersoner. En biobank opfattes som et manuelt register og er derfor i de fleste tilfælde omfattet af persondatalovens krav.

Hvis biologisk materiale opbevares ud over den tid, det tager at indsamle og analysere prøverne, er der tale om en biobank, mens prøver, der destrueres umiddelbart efter endt analyse, ikke er omfattet af biobankbegrebet.

Dog er det sådan, at biologisk materiale, der anvendes i forbindelse med et privat forskningsprojekt, er omfattet af persondataloven, men projektet skal ikke anmeldes til Datatilsynet.

[102] Persondataloven, §5

For forskningsbiobanker, hvor det biologiske materiale er indsamlet til fremtidig brug, dvs. at der ikke er tale om, at det indgår i et konkret forskningsprojekt, skal der både i offentligt og privat regi foretages anmeldelse til Datatilsynet. For regioner og statslige myndigheder, der behandler personoplysninger i forbindelse med biobanker, der udelukkende anvendes til videnskabelige eller statistiske formål, skal der kun foretages en samlet anmeldelse, og ikke anmeldelse for hver enkelt forskningsbiobank. Et eksempel på en sådan biobank er Danmarks Nationale Biobank på Statens Seruminstitut.

Biologisk materiale indeholder følsomme personoplysninger, der med forskellige teknikker kan bestemmes og beskrives. Biologisk materiale indeholder desuden altid flere oplysninger, end de oplysninger, der skal indgå i den aktuelle forskning. Det er derfor vigtigt, at man sikrer sig mod, at uvedkommende kan få kendskab til eller misbruge oplysningerne, bl.a. ved at det biologiske materiale opbevares i en ikke umiddelbart personhenførbar form og at nøglerne til at koble personoplysninger sammen med det biologiske materiale opbevares særskilt og uden for det it-miljø, der anvendes i relation til håndtering af prøvematerialet.

Såfremt biologisk materiale opbevares CPR-nummer, navn e.l., skal der træffes særlige sikkerhedsforanstaltninger.

I forhold til konkrete forskningsprojekter gælder det, at materialet skal destrueres eller anonymiseres, når projektet er afsluttet.

8.5 Opbevaring og logning

Data skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til personoplysninger[103].

For offentlige myndigheder er kravene beskrevet i sikkerhedsbekendtgørelsen og uddybes i den vejledning til sikkerhedsbekendtgørelsen, som man også kan finde på Datatilsynets hjemmeside. Her kan man finde de konkrete krav til adgangsstyring, fysisk sikkerhed, logning m.v.

Alle dataansvarlige offentlige myndigheder skal have udarbejdet interne uddybende sikkerhedsregler i forhold til sikkerhedsbekendtgørelsen[104]. Man skal derfor inden projektets igangsættelse sikre sig, at man overholder retningslinjerne hos den pågældende myndighed.

Inden man igangsætter et projekt, er det derfor vigtigt at sikre sig, at de databaseværktøjer og programmer, man anvender til behandling af data, lever op til sikkerhedsbekendtgørelsens krav.

[103] Persondataloven, §41, stk. 3

[104] Sikkerhedsbekendtgørelsen, §5

For offentlige myndigheder er der i sikkerhedsbekendtgørelsen krav om, at man kan logge, hvilke personer, der har haft adgang til personoplysninger.

Hvis oplysningerne opbevares i direkte personhenførbar form, f.eks. med et CPR-nummer, skal logningen omfatte tidspunkt, bruger, brugerens anvendelser, angivelse af person, oplysningerne vedrører eller anvendt søgekriterium[105].

Hvis behandlingen af personoplysninger sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikations-oplysninger forinden er krypteret eller erstattet af kodenummer e.l., skal logningen kun omfatte tidspunkt og bruger[106].

Mange af de generelle værktøjer, der anvendes til statistikformål, f.eks. Excel og Access, opfylder ikke sikkerhedsbekendtgørelsens krav, og man skal også være opmærksomme på, hvilke logningskrav, de forskellige statistikprodukter kan leve op til.

Hvis systemet kun kan logge tidspunkt og bruger, skal personoplysninger som minimum pseudonymiseres. Hvis systemet heller ikke kan logge dette, skal alle oplysninger være anonymiserede.

8.6 Videregivelse til andre forskningsprojekter

Personoplysninger, der behandles i forbindelse med en videnskabelig eller statistisk undersøgelse må ikke anvendes til andre formål end dem, de er indsamlet til. Der må alene ske videregivelse til andre videnskabelige eller statistiske undersøgelser, for hvilke oplysningerne er nødvendige, men det kræver en særlig tilladelse fra Datatilsynet.

Sker der ændringer til et eksisterende forskningsprojekt, skal dette altid anmeldes til Datatilsynet. Er der tale om væsentlige ændringer, som f.eks. ændringer af selve formålet med behandlingen eller nye påtænkte overførsler af oplysninger til tredjelande, skal dette godkendes af Datatilsynet, inden ændringen kan træde i kraft. Ved mindre ændringer, f.eks. skift til en ny databehandler, skal dette anmeldes senest 4 uger efter, at det er trådt i kraft, jf. kapitel 4.

Hvis den samme dataansvarlige vil anvende data fra et eksisterende forskningsprojekt i et nyt projekt inden for den dataansvarliges ansvarsområde, er der tale om genanvendelse af data. Inden data kan overlades, skal der hos den dataansvarlige tages stilling til, om de ønskede data er nødvendige for det nye projekt. Endvidere skal det nye projekt være anmeldt til Datatilsynet forinden eller indgå i myndighedens paraplyanmeldelsen for videnskabelige og statistiske undersøgelser.

Datatilsynet har den 12. juni 2015 meddelt regionerne generelle tilladelser til at videregive oplysninger omfattet af myndighedens paraplyanmeldelse vedrørende sundhedsvidenskabelig forskning og kliniske kvalitetsdatabaser, der er godkendt af Sundhedsdatastyrelsen. Det omfatter dog ikke videregivelse af biologisk materiale og

[105] Sikkerhedsbekendtgørelsen, §19, stk 1

[106] Sikkerhedsbekendtgørelsen, §19. stk.4.

omfatter kun videregivelse til dataansvarlige, der er etableret i Danmark. Datatilsynet har i den forbindelse fastsat en række standardvilkår. For at sikre, at standardvilkårene overholdes skal der internt i regionen indhentes en godkendelse, inden videregivelsen sker. Det sker ved henvendelse til myndighedens kontaktperson til Datatilsynet.

8.7 Offentlig eller privat forskning

Hvis et forsknings- eller statistikprojekt foretages for en offentlig myndighed, kan projektet ikke betragtes som et privat projekt.

En del offentlige myndigheder har fastlagt retningslinjer for, at forsknings- og statistikprojekter, der involverer data eller ressourcer, som de har ansvaret for, skal anmeldes som offentlige. Inden man igangsætter et projekt, skal man derfor sikre sig, at det sker i overensstemmelse med myndighedens regelsæt.

8.8 Pseudonymisering og anonymisering

Ved etableringen af et forskningsprojekt skal man overveje, hvordan man sikrer følsomme personoplysninger, der indgår i projektet. I Danmark har anvendelsen af CPR-nummeret gjort det nemt at sammenholde data fra forskellige kilder på den enkelte person, men det betyder samtidig, at der stilles store krav til at beskyttelse af oplysningerne, både teknisk og organisatorisk.

Derfor skal det altid overvejes, om der er behov for at kende identiteten på de personer, der indgår i ens projekt, eller om man kan skjule eller fjerne personidentifikationen.

8.8.1. Pseudonymisering

Ved pseudonymisering forstås, at identifikatorer (såsom navn og CPR-nummer) ændres, enten ved hjælp af kryptering eller ved erstatning af identifikationsoplysninger med id-nr., således at modtageren af oplysningerne ikke umiddelbart er i stand til at identificere den registrerede.

Ved pseudonymisering er det stadig muligt at sammenstille data på tværs af registre, og i og med, at afsenderen stadig har nøglen til at re-identificere en person, er pseudonymiserede data stadig omfattet af persondatalovens krav.

8.8.2 Anonymisering

Ved anonymisering fjernes så mange oplysninger om personens identitet, at personen ikke længere direkte eller indirekte kan identificeres.

Med anonymisering er data ikke længere personhenførbare og derfor ikke omfattet af persondatalovens krav, dog under forudsætning af at der er taget de nødvendige forholdsregler i forhold til diskretionering.

Selv om et forskningsprojekt er baseret på anonyme data, skal man være sig bevidst om, at sammensætning af forskellige informationer kan føre til, at man kan identificere en person derudfra.

Hvis man eksempelvis ser på antallet af aborter blandt kvinder i aldersgruppen 15-25 år pr. kommune, så vil man i meget små kommuner som f.eks. Læsø med ca. 1800 beboere måske komme ned på et antal, som gør, at man entydigt kan identificere personen eller personerne.

I sådanne tilfælde er det nødvendigt, at ens datasæt diskretioneres. Der findes forskellige metoder til diskretionering.

Det kan enten ske ved gruppering, hvor man grupperer værdierne på et niveau, der umuliggør genkendelse eller ved trunkering, hvor man afskærer yderværdier kan ofte være nødvendig for at undgå genkendelse.

En anden metode er, at en tabel med kombination af mange variabler kan opdeles i flere tabeller.

Hvis det sker, skal det sikres, at der ikke er utilsigtede indirekte links via variabelværdier mellem tabellerne.

Endelig kan man, hvis ikke andet er muligt, udelade observationer fra tabellen. I så fald kan det være nødvendigt med konsekvensudeladelser af andre observationer for at undgå en mulighed for at deducere sig frem til den udeladte observation.

Det er altid den dataansvarlige, der har ansvar for at sikre, at der er foretaget den nødvendige diskretionering af et datasæt.

I forbindelse med sammensætningen af en stikprøvepopulation, anbefales det, at udvalgskriterier ikke indeholde følsomme oplysninger, f.eks. en diagnosekode e.l. Stikprøvestørrelsen fastlægges bl.a. under hensyntagen til stikprøveusikkerheden, men udvalgskriterierne skal være fastlagt så bredt, at udvalgssandsynligheden for den enkelte, person i gruppen ikke overstiger 10 pct. Hvis kravet til stikprøvens størrelse er 1.000 personer, så skal den population, hvorfra stikprøven trækkes, være på mindst 10.000 personer.

8.9 Big data

Big Data er et begreb inden for datalogi, der bredt dækker over indsamling, opbevaring, analyse, processering og fortolkning af enorme mængder af data.

I mange sammenhænge fremhæves mulighederne for at kunne sammenstille store datamængder som en mulighed for at skabe nye forretningsmuligheder, kvalitetssikre patientbehandling, forbedre forebyggelse af livsstilssygdomme o.l.

Behandling af personoplysninger i forbindelse med Big Data skal ske under iagttagelse af persondatalovens regler.

9. Overførsel af patientoplysninger til EU- og tredjelande

Persondataloven er implementeringen af EU's persondatadirektiv i dansk lov. Persondatadirektivet skal på den ene side beskytte de borgere, hvis oplysninger bliver behandlet og på den anden side sikre fri udveksling af sådanne oplysninger inden for EU.

Personoplysninger kan således videregives til dataansvarlige eller overlades til databehandlere i andre EU-lande, så længe man overholder reglerne i persondataloven og at anden relevant lovgivning samt det pågældende lands lovgivning på området Det vil sige, at hvis det drejer sig om patientoplysninger, så skal reglerne i sundhedsloven også overholdes.

Når man vil overføre personoplysninger til det, der kaldes tredjelande, skal man sikre, at de bliver beskyttet på et niveau, der svarer til kravene i persondataloven og at man efterlever kravene i lovens § 27 vedr. overførsel til tredjelande.

Med tredjelande forstås lande uden for EU og EØS. EØS-landene Norge, Island og Lichtenstein opfattes ikke som tredjelande.

Nogle tredjelande er af EU-Kommissionen vurderet som lande, der generelt enten via lovgivningen eller via andre foranstaltninger sikrer et tilstrækkeligt beskyttelsesniveau (sikre tredjelande). Det gælder f.eks. Færøerne og Schweiz. EU-Kommissionen vurderer, at de lande, der er godkendt som sikre tredjelande generelt enten via lovgivning eller via andre foranstaltninger sikrer et tilstrækkeligt beskyttelsesniveau.

Når der er tale om sikre tredjelande, skal der ikke indhentes tilladelse fra Datatilsynet, hvis det er en offentlig myndighed, der er dataansvarlig, mens der ved privates overførsel til sikre tredjelande skal indhentes tilladelse, hvis der overføres følsomme oplysninger.

Offentlige myndigheder skal, såfremt der er tale om en databehandler i et sikkert tredjeland, som altid indgå en databehandleraftale med denne. Hvis der er tale om

videregivelse til en anden dataansvarlig, skal dette godkendes af Datatilsynet og fremgå af anmeldelsen.

Ved overførsel af personoplysninger til usikre tredjelande, f.eks. USA og Grønland, kan overførsel ske med indgåelse af en af EU-Kommissionens standardkontrakter.

Hvis der er foretaget ændringer i ordlyden i forhold til EU-Kommissionens standardkontrakter, skal der indhentes tilladelse fra Datatilsynet til overførslen. Datatilsynet skal underrette EU-Kommissionen om sådanne eventuelle tilladelser.

Hvis data overføres fra en del af en virksomhed, der er placeret inden for EU, til en del af virksomheden, der ligger uden for EU, kan dette ske, hvis virksomheden har udarbejdet det, der hedder bindende virksomhedsregler. Med bindende virksomhedsregler tilkendegives det, at man overholder det nødvendige beskyttelsesniveau i alle dele af virksomheden.

Safe Harbor ordningen, hvor et firma i USA eller et andet land anmelder til ordningen, at de sikrer det krævede beskyttelsesniveau, kan ikke længere anvendes. EU-Domstolen har den 6. oktober 2015 konkluderet, at ordningen er i strid med Databeskyttelsesdirektivet, fordi den ikke sikrer det nødvendige beskyttelsesniveau. Derfor skal man bruge et andet retligt grundlag for at overføre data, f.eks. EU-kommissionens standardkontrakter som beskrevet ovenfor.

EU-kommissionen har d. 2. februar 2016 indgået en politisk aftale med USA om et nyt rammeværk for transatlantiske udveksling af personoplysninger under navnet EU-U.S Private Shield. Den nye aftale indeholder mere bindende forpligtelser for virksomheder, der håndterer personoplysninger for EU-borgere, klare beskyttelses- og gennemsigtighedskrav for den amerikanske stats adgang til personoplysninger og en mere effektiv beskyttelse af EU-borgernes rettigheder med forskellige klagemuligheder.

Det næste skridt vil være, at de amerikanske virksomheder skal registrere sig på Private Shield-listen og erklære, at de lever op til de beskrevne krav.

9.1 Krigsregelen

Hvis man anvender en databehandler i et andet land, skal der indgås en databehandleraftale på sammen måde, som hvis der er tale om en dansk databehandler.

Anvender man en databehandler i et andet land, skal man vurdere, om de oplysninger, der behandles er omfattet af den såkaldte "krigsregel"107, hvor der står:

"For oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal der træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold. "

[107] Persondataloven, § 41, stk. 4,

Reglen indebærer, at ikke alle behandlinger af personoplysninger vil kunne udføres af en databehandler i et andet land.

Hvis man er i tvivl om, hvorvidt databehandlingen, som ønskes varetaget af en databehandler i et andet land, er omfattet af krigsregelen, kan man henvende sig til Datatilsynet.

I forhold til anvendelsen af cloud-løsninger skal man ligeledes være opmærksom på krigsregelen, da leverandører af cloud-løsninger, med mindre andet er aftalt, kan placere data på flere servere i flere lande.

9.2. Særligt vedr. videnskabelige og statistiske undersøgelser

Hvis der er tale om videregivelse af oplysninger til brug for videnskabelige eller statistiske undersøgelser til en dataansvarlig i et tredjeland, skal man som supplement til ovenstående regler indhente en godkendelse fra Datatilsynet inden overførslen finder sted, jf. persondatalovens §10, stk. 3, på samme måde som det gælder, hvis der er tale om en dataansvarlig i Danmark.

Reglerne gælder også for sundhedsfaglig forskning, som udføres i samarbejde med forskere i andre lande.

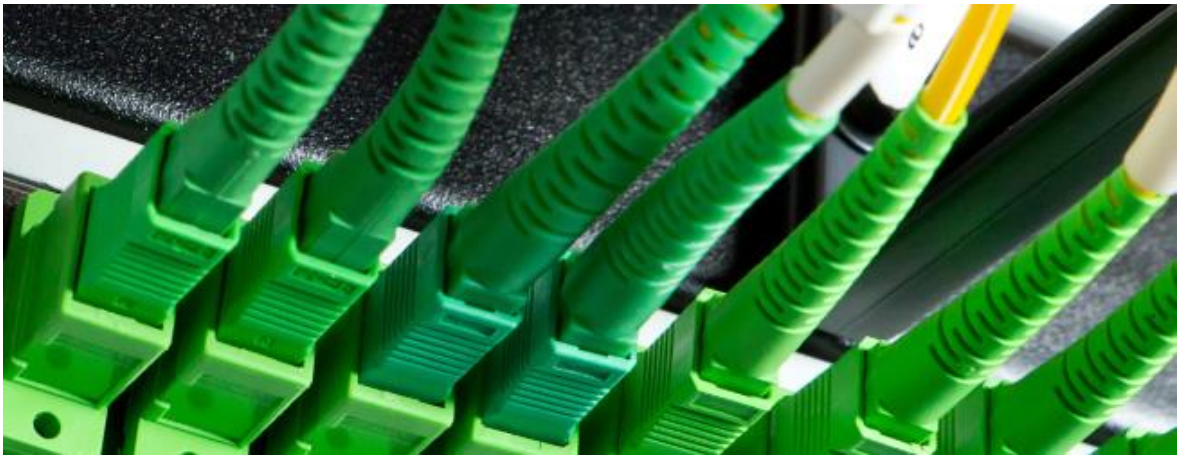
Hvis forskere fra andre lande behandler data på vegne af en dataansvarlig person eller myndighed, skal der udarbejdes en databehandleraftale og hvis der er tale om en samarbejdspartner i et usikkert tredjeland, så skal der foreligge en EU standardkontrakt.

9.2 Beskyttelse af personoplysninger ved rejse i udlandet

Hvis man på rejse i udlandet har personoplysninger eller fortrolige oplysninger lagret på sin PC eller har fjernadgang til følsomme oplysninger, skal man være opmærksom på og sikre sig imod, at uvedkommende kan få adgang til disse oplysninger. Dette kan man sikre sig imod med kryptering af data og adgangskontrol.

Man skal altid sørge for at have sit it-udstyr under opsyn og man skal undgå at anvende offentlige internetopkoblinger til at udveksle eller tilgå følsomme personoplysninger.

Center for Cybersikkerhed har udgivet en sikkerhedsanbefaling "IT-sikkerhed på rejsen", hvor man kan læse mere om, hvordan man beskytter fortrolige og følsomme oplysninger på rejser.



10. Netværkssikkerhed

Øget samarbejde mellem parterne i sundhedsvæsenet betyder også, at der er behov for at kunne kommunikere fortrolige og følsomme personoplysninger på tværs af organisationer.

Det er derfor vigtigt, at man kender risici og muligheder, når man skal kommunikere med andre parter.

I persondataloven[108] fremgår det, at den dataansvarlige skal træffe de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller behandles i strid med loven.

Det indebærer, at personoplysninger også ved transmission på et net skal sikres mod disse risici.

10.1 Intern kommunikation

Det kan i praksis være svært for almindelige medarbejdere at afgøre, hvorvidt et netværk er "åbent" eller "lukket". Tidligere foregik kommunikationen typisk inden for et fysisk begrænset område, hvor ens lokale netværk var fysisk isoleret fra andre net.

I dag er der sjældent denne tekniske afgrænsning. De fleste organisationer har etableret et trådløst netværk, og der er etableret adgang til andre lokale netværk, f.eks. hos samarbejdspartnere eller eksterne leverandører.

Datatilsynet har udarbejdet en it-sikkerhedstekst vedr. datatransmission af personoplysninger på åbne net. Heri anbefales det, at den dataansvarlige foretager en

[108] Persondataloven, §41, stk. 3

vurdering af netværkets "åbenhed". Ud fra en række indikatorer kan det afgøres, i hvor høj grad man selv som dataansvarlig har styr på datastrømmen.

Hvis man som medarbejder er i tvivl om, hvorvidt de personoplysninger, man vil sende, vil blive transmitteres på et åbent net, anbefales det, at man sikrer kommunikationen ved at sende oplysningerne som krypteret e-mail.

10.2 Ekstern kommunikation

Har man brug for at dele oplysninger med en sundhedsperson i en anden organisation, skal man altid overveje, om disse oplysninger er fortrolige eller følsomme. Når der er tale om patientoplysninger, er det næsten altid tilfældet og man skal derfor sikre sig, at oplysningerne er beskyttet med stærk kryptering under transporten fra afsender til modtager.

10.2.1 Internettet

Når offentlige myndigheder kommunikerer via internettet og kommunikationen indeholder fortrolige eller følsomme oplysninger, skal oplysningerne krypteres og brugeren skal være autentificeret med tofaktor-autentifikation Med tofaktor-autentifikation menes et system, hvor brugeren autentificeres ved hjælp af mindst to faktorer, noget de ved og noget de har. Det man har, kan eksempelvis være en hemmelig softwarenøgle eller noget fysisk så som en token, et papirnøglekort, som det, der anvendes i NemID eller en kode, der sendes til ens mobiltelefon. I Datatilsynets it-sikkerhedstest nr. 1 kan man finde yderligere eksempler på, hvordan man kan etablere flerfaktor-login-

Dette kan eksempelvis sikres ved at anvende sikker e-mail, hvor man med digital signatur eller NemID sikrer, at oplysninger i mailen er krypteret og at mailen er signeret.

I kommuner og på sygehuse er der ofte allerede etablerede sikre postkasser, som kan anvendes, hvis man har behov for at sende fortrolige eller følsomme oplysninger.

Datatilsynet har ikke opsat samme regler for privates e-mail kommunikation over internettet, men det anbefales, at private, f.eks. privatpraktiserende læger, beskytter personoplysninger, når de kommunikerer via internettet.

Datatilsynet har dog stillet udtrykkeligt krav om kryptering, når der sker

- overførsel af **følsomme** oplysninger via hjemmesider
- overførsel af **personnumre** via hjemmesider, samt i
- tilfælde, hvor behandlingen af personoplysninger i den private sektor sker efter tilladelse med **vilkår** om konkrete sikkerhedsforanstaltninger ved transmission over internettet.

Hvis en offentlig myndighed kommunikerer med en borger via internettet, skal det ske krypteret til dennes digitale postkasse. Offentlige myndigheder må ikke, selv om

borgeren giver tilsagn til det, sende fortrolige eller følsomme oplysninger som almindelig e-mail.

> Fortrolige eller følsomme personoplysninger må aldrig sendes med almindelig e-mail.

Mellem nogle organisationer har man valgt at etablere sikrede (TSL 1.2) tunneller, som etableres bilateralt mellem 2 organisationer.

Hvis man er i tvivl om, hvilke løsninger, ens organisation har etableret til at sende sikker e-mail, kan man kontakte it-afdelingen.

10.2.2 Sundhedsdatanettet

Sundhedsdatanettet (SDN) har eksisteret siden 2003. Sundhedsdatanettet er et sikret netværk som står til rådighed for alle parter i sundhedssektoren, der har brug for at kommunikere patientoplysninger o.l. til andre parter. Med sundhedsdatanettet er det for eksempel muligt at foretage opslag i eksterne databaser, udveksle oplysninger eller billeder eller afholde videokonferencer.

Hertil kommer, at den fællesoffentlige sundhedsportal sundhed.dk benytter sundhedsdatanettet som forbindelseskanal til at hente de oplysninger fra forskellige sundheds it-systemer, som vises for borgere og sundhedspersoner på portalen.

> *VAN (Value Added Network) er en ældre teknologi, der i stort omfang bruges til at udveksle MedCom-meddelelser.*

På den måde supplerer sundhedsdatanettet det VANS-baserede sundhedsdatanet, der i stor skala anvendes til tværsektoriel udveksling af XML- og EDIFACT-meddelelser.

Filosofien bag sundhedsdatanettet er, at sundhedssektorens parter skal kunne få opfyldt deres kommunikationsbehov via én og samme netværksforbindelse. Nettet er på den måde det elektroniske samlingspunkt for kommunikationen i sundhedsvæsenet, uanset om brugerne hører hjemme i den offentlige eller private sektor.

For at blive koblet op på sundhedsdatanettet skal brugeren have en formel godkendelse hos MedCom.

En række aktører er dog forhåndsgodkendt. Det drejer sig om alle regioner, offentlige og private sygehuse, praksisydere under den offentlige sygesikring, kommuner, apoteker og private laboratorier. Hertil kommer IT-leverandører, der anvendes af og anbefales af ovenstående parter.

Sundhedsdatanettet består af et centralt knudepunkt[109] og et MPLS-net. For at blive tilsluttet sundhedsdatanettet skal der etableres en forbindelse til nettet fra ens eget, sikrede netværk, fx regionsnet.

Da der som oftest er tale om følsomme personoplysninger, der kommunikeres, anbefales det, at de dataansvarlige/serviceudbyderne anvender endepunktskryptering (SSL/TLS) mellem server og klient, så udefra kommende ikke kan få adgang til oplysningerne. Datatilsynet har i sin it-sikkerhedstekst 2 flere anbefalinger i forhold til at sikre mod, at personoplysninger kommer til uvedkommendes kendskab i forbindelse med datatransmission.

10.3 Den nationale serviceplatform

Via sundhedsdatanettet kan man bl.a. få adgang til Den Nationale Serviceplatform (NSP)[110].

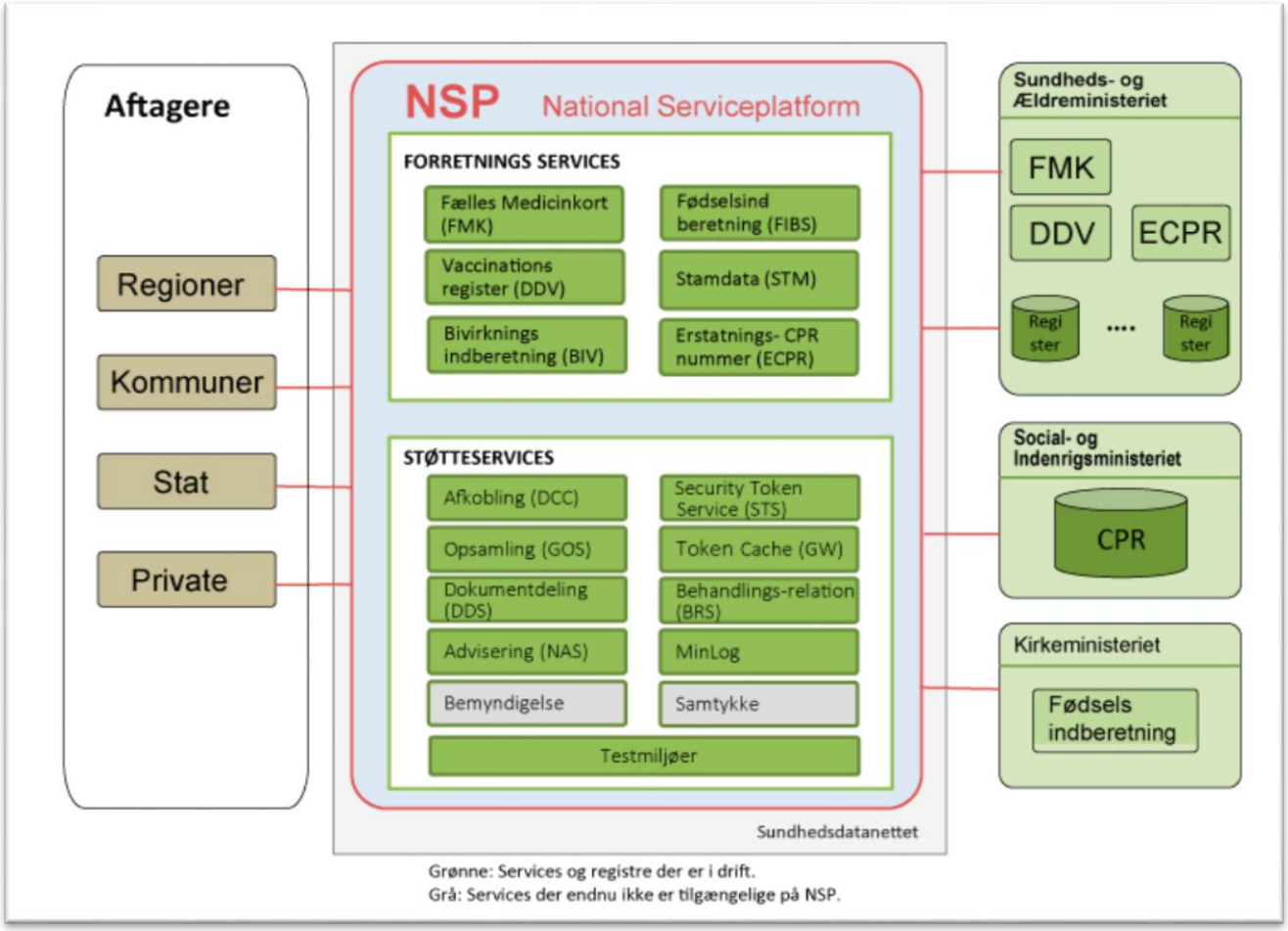
> NSP, den nationale serviceplatform, udstiller en række oplysninger til brug for sundhedsvæsenet: CPR-oplysninger, SOR (Sundhedsvæsenets organisationsregister) og andre klassifikationer. Adgang til det fælles medicinkort sker også via NSP.

Formålet med den nationale serviceplatform er at stille en infrastruktur til rådighed, som sammen med sundhedsdatanettet sørger for en sikker og robust adgang til fælles nationale registre og services, som anvendes til planlægning og registrering af oplysninger i forbindelse med patientbehandlingen.

[109] Læs mere på http://medcom.dk/wm110009

[110] Læs mere på nspop.dk

Den nationale serviceplatform giver adgang til et landsdækkende CPR-register, til Det fælles Medicinkort samt en række klassifikationer og services, som kan anvendes af parterne i sundhedsvæsenet.



Figur 10.1 Den nationale serviceplatform.

Services på NSP tilgås ved system-til system-integration via webservices. Det betyder, at det ikke er muligt at tilgå services på NSP, medmindre man har en "klient" – et program – som kan koble op til NSP og udveksle data med services på NSP.

Teknisk er det et krav til de organisationer, der ønsker at få adgang til NSP, at de tilgår NSP via Sundhedsdatanet, og at brugeren er autentificeret ved anvendelse af et medarbejdercertifikat (MOCES).

Der er *administrativt* krav om, at der er indgået aftale med Sundhedsdatastyrelsen om anvendelse af konkrete services.

11. Mobil sikkerhed

I takt med, at man i højere og højere grad kan modtage, sende, lagre og tilgå information på mange forskellige former for udstyr, bliver det mere vigtigt at sikre sig, at fortrolige eller følsomme oplysninger kan behandles med brug af dette udstyr uden at det kompromitterer datasikkerheden.

11.1 Hvad er mobile enheder?

Mobile enheder er mange forskellige ting, men tendensen er, at de bliver mere avancerede og at de typisk har en netadgang, som gør dem mere sårbare overfor f.eks. malware, hvis de ikke er sikrede tilstrækkeligt.

Mange anvender i dag smartphones, tablets eller bærbare PC-er i deres arbejde, også i sundhedsvæsenet, og der er derfor behov for øget opmærksomhed på de trusler, der specielt retter sig mod mobilt udstyr og de løsninger, der kan være med til at højne sikkerhedsniveauet.

Samtidig går udviklingen mod, at der er indbygget små computere i alt – ure, sko, kameraer og stikdåser – det der i it-verdenen omtales som Internet of Things. Der bliver derfor flere muligheder for at trænge ind og skaffe sig oplysninger om privatpersoner og organisationer, og det kan være svært sikkerhedsmæssigt at følge med den tekniske udvikling, også fordi sikkerhed generelt ikke prioriteres særligt højt af leverandørerne af apps.

Det er derfor vigtigt, at man i sundhedsvæsenet foretager en risikovurdering af anvendelse af forskellige former for mobilt udstyr, hvor man vurderer, om det er muligt at etablere sikringstiltag, som er tilstrækkelige i forhold til behovet for at beskytte de oplysninger, man vil behandle eller kommunikere.

11.2 Trusler

Mobilt udstyr er grundlæggende udsat for de samme trusler som alt andet it-udstyr, men i og med at de ofte anvendes i mindre beskyttede miljøer, har mobile enheder nogle yderligere sårbarheder.

Mobile enheder er mere udsatte for at blive stjålet end en stationær arbejdsstation, der befinder sig på arbejdspladsen.

Hvis enheden ikke er beskyttet med adgangskode og/eller kryptering, øges risikoen for, at uvedkommende kan få adgang til de oplysninger, der er lagret på enheden.

Der kan også meget let ske tab af data, hvis de er lagret på en mobil enhed, hvor der typisk ikke tages back up.

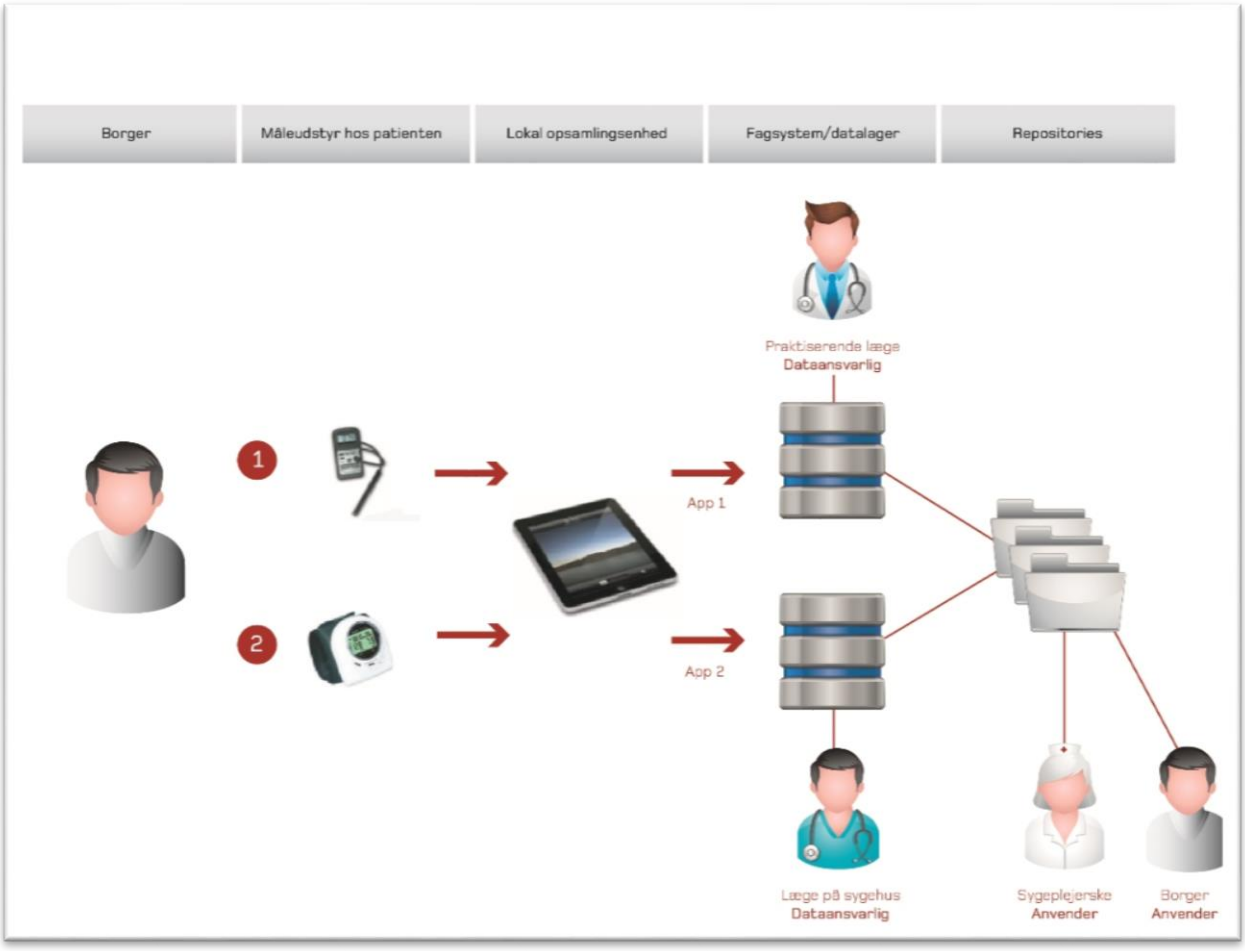
Malware kan ligesom på en PC komme ind på den mobile enhed på mange forskellige måder, f.eks. gennem et link eller en vedhæftet fil i ens mailprogram, når man downloader og installerer programmer (apps), via SMS/MMS eller sociale medier som Facebook o.l.

Endelig kan man risikere, at andre kan opsnappe ens kommunikation med et såkaldt snifferprogram, hvis man bruger sin mobile enhed på et åbent trådløst netværk, f.eks. i toget eller i lufthavnen.

11.3 Løsninger

Hvis man ønsker at anvende mobilt udstyr til at indsamle, lagre eller kommunikere sundhedsoplysninger, f.eks. i forbindelse med et telemedicinsk projekt e.l., skal den dataansvarlige sikre sig, at det anvendte udstyr og anvendte Apps overholder sikkerhedsbekendtgørelsens krav.

Det betyder, at hvis data lagres på den mobile enhed, skal data være krypteret og der skal være adgangskontrol til enheden. Hvis data kommunikeres via den mobile enhed, f.eks. måleresultater fra måleudstyr, der via en telefon eller tablet sendes til en database hos den dataansvarlige som vist i nedenstående figur, så skal kommunikationen foregå krypteret.



Figur 11.1 Opsamling af helbredsdata hos borgeren. OBS: For lægen på sygehuset er det en region, der er dataansvarlig, ikke lægen selv. Kilde: Referencearkitektur for opsamling af helbredsdata hos borgeren, NSI 2013.

Hvis det er borgerens eget udstyr, der anvendes til opsamling af helbredsoplysninger, som anvendes af en sundhedsperson, kan man ikke nødvendigvis sikre, at den mobile enhed har det sikkerhedsniveau, som er påkrævet. I disse tilfælde skal den dataansvarlige sørge for, at det program eller den app, der anvendes til at behandle oplysningerne, har de nødvendige sikringstiltag indbygget.

Hvis man ikke vil sikre data på udstyr eller i apps i henhold til sikkerhedsbekendtgørelsen, kan man vælge at kode de oplysninger, der kommunikeres, så de først gøres personhenførbare, når de registreres i et sikret miljø hos den dataansvarlige.

Hvis mobilt udstyr anvendes som arbejdsredskab i sundhedsvæsenet, herunder til behandling af personoplysninger, bør man anvende enheder, som kan administreres centralt med et MDM-system, så det sikres, at der sker opdatering af malwarebeskyttelse, styring af adgangskode på enheden, opdatering af operativsystem, begrænsning af brugers rettigheder m.v. og at indhold kan slettes, hvis enheden bliver stjålet. Når man kommunikerer følsomme oplysninger med anvendelse af mobile enheder, bør den sættes op til kun at kunne anvende den sikrede e-mail-funktion og browserfunktion, som er valgt i ens organisation, og apps bør kun kunne installeres gennem et app-katalog, der stilles til rådighed i organisationen. Der skal altid anvendes to-faktorautentifikation, f.eks. digital signatur, jf. Datatilsynets afgørelse vedr. politiets indberetning af personoplysninger til Erhvervs- og selskabsstyrelsen med anvendelse af brugernavn og password.

MDM – Mobile Device Management anvendes til at sikre og overvåge mobile enheder.

Hvis medarbejdere har tilladelse til at bruge deres egne mobile enheder, det der kaldes BYOD (Bring Your Own Device), bør der ligeledes opstilles retningslinjer for, hvilke sikringstiltag, der skal være etableret, herunder f.eks. om enheden skal være underlagt arbejdspladsens MDM-system.

12. Krav vedr. informationssikkerhed

Digitaliseringen betyder, at vi i højere grad bliver afhængige af de it-løsninger, som understøtter det daglige arbejde både i den private og den offentlige sektor, og samfundet som sådan bliver derfor også mere sårbart over for trusler, der påvirker tilgængelighed, fortrolighed eller integriteten i de oplysninger, der ligger til grund for vores arbejde.

Det er derfor vigtigt, at der er fokus på at beskytte data og systemer, både hos den forretningsmæssige ledelse, i it-afdelingen og hos medarbejderne.

12.1 Informationssikkerhed er mere end it-sikkerhed

Informationssikkerhed gælder ikke kun for oplysninger, der opbevares i forskellige it-løsninger, men handler også om oplysninger på papir, billeder, video m.v.

Det er derfor vigtigt, at man også tænker på den fysiske sikkerhed for, at f.eks. uvedkommende ikke kan få adgang til fortrolige oplysninger. Man skal derfor ved indretning af lokaler, hvor der kommer patienter og pårørende, være opmærksom på, hvordan man placerer printere, skærme, storskærme og oversigtstavler, så de ikke giver mulighed for, at uvedkommende kan skaffe sig oplysninger, de ikke er berettigede til at se.

12.2 Anvendelse af standard for informationssikkerhed

Siden 2014 har statslige institutioner været forpligtet til at efterleve den standard for informationssikkerhed, som hedder ISO/IEC 27001.

Formålet med standarden er at sikre, at man i den enkelte organisation får håndteret alle de områder, som er nødvendige for at man kan etablere det nødvendige sikkerhedsniveau både i forhold til, hvor vigtig it-understøttelsen er for opgavevaretagelsen og i forhold til, hvor fortrolige eller følsomme, de oplysninger, der behandles, er.

Der er ikke krav om, at private efterlever kravene i ISO27001, men eftersom anvendelsen af it i sundhedsvæsenet er stigende og der i højere grad er et samarbejde på tværs mellem parterne, anbefales det at tage udgangspunkt i standarden for at sikre, at it-løsningerne i ens egen organisation ikke er med til at kompromittere sikkerheden generelt.

For kommunale og regionale myndigheder er det aftalt i digitaliseringsstrategien 2016-2020, at de skal følge principperne i ISO27001 inden for de første tre år af strategiperioden.

Anvendelse af standarden skal tilpasses den enkelte organisation. Der kan være forskel på, hvad der er nødvendigt og hensigtsmæssigt for at have et tilstrækkeligt sikkerhedsniveau, alt efter størrelse og type af organisation. Det er vigtigt at afveje krav til informationssikkerhed i forhold til andre krav, herunder økonomiske forhold, men det vil være hensigtsmæssigt, at disse vurderinger dokumenteres.

Standarden indeholder en række kontrolmål, der dækker følgende områder:

- A.5 Informationssikkerhedspolitikker
- A.6 Organisering af informationssikkerhed
- A.7 Personalesikkerhed
- A.8 Styring af aktiver
- A.9 Adgangsstyring
- A.10 Kryptografi
- A.11 Fysisk sikring og miljøsikring
- A.12 Driftssikkerhed
- A.13 Kommunikationssikkerhed
- A.14 Anskaffelse, udvikling og vedligeholdelse af systemer
- A.15 Leverandørforhold
- A.16 Styring af informationssikkerhedsbrud
- A.17 Informationssikkerhedsaspekter vedr. nød-, beredskabs- og reetableringsstyring
- A.18 Overensstemmelse

Digitaliseringsstyrelsen har udgivet flere vejledninger, som kan understøtte organisationens implementering af ISO27001-standarden, herunder en guide til implementering af ISO27001.

12.2.1. Ledelsesværktøj

ISO27001 lægger vægt på, at det er organisationens øverste ledelse, der har ansvaret for informationssikkerhed i organisationen. Det er ledelsen, der har ansvaret for at fastlægge et passende risiko- og sikkerhedsniveau samt prioritere ressourcer og sikkerhedsaktiviteter

Det er derfor vigtigt, at man får organiseret arbejdet med informationssikkerhed, så ledelsen har den nødvendige viden til at træffe beslutninger.

12.2.2. Risikovurdering

Standarden tager udgangspunkt i, at organisationens ledelse vurderer, hvilke trusler og risici, man skal forholde sig til. Ud fra forretningsprocesserne skal der tages stilling til, hvilke konsekvenser et brud på sikkerheden kan få for organisationen.

Igennem en risikovurdering identificeres og analyseres trusler og sårbarheder og hvor stor sandsynlighed og risiko, der er for tab af fortrolighed, integritet og tilgængelighed.

Risikovurderingen skal give mulighed for at vurdere, hvilke trusler, der er mest sandsynlige og mest risikable i forhold til, at organisationen kan udføre sine opgaver og nå sine mål. Hermed har ledelsen et værktøj til at prioritere indsatsen, så organisationen opnår et passende niveau for informationssikkerhed.

F.eks. skal en praktiserende læge vurdere, hvor længe han vil kunne arbejde uden adgang til sit lægepraksissystem. Herefter vurderes det, hvor stor sandsynligheden er for, at systemet er utilgængeligt i et tidsrum, der er længere end accepteret. På baggrund af oplysninger om konsekvens og sandsynlighed vurderes det så, hvilke sikringstiltag, der er nødvendige for at bringe risikoen for et længerevarende nedbrud ned på et acceptabelt niveau.

Udover at man løbende skal vurdere trusler og sårbarheder i sine eksisterende it-løsninger er det rigtig vigtigt, at man fra starten af et it-projekt foretager en risikovurdering, så man kan få stillet de rigtige krav vedr. informationssikkerhed til leverandørerne.

12.3 Cybersikkerhed

I de seneste år er der kommet yderligere fokus på de trusler, der kommer fra internettet såsom malware og muligheden for hackerangreb. Tidligere blev de it-systemer, der indeholdt organisationens fortrolige eller følsomme data, primært anvendt inden for ens egen organisation og kunne beskyttes på en helt anden måde end i dag, hvor data i langt højere grad udveksles mellem de parter i sundhedsvæsenet, som deltager i behandlingen af en patient.

Derfor er alle organisationer blevet mere udsatte for trusler fra internettet, og angrebsmetoderne er blevet mere sofistikerede og svære at opdage og undgå. Dette skyldes bl.a., at både kriminelle organisationer og nogle landes efterretningsvæsener bruger internettet til at skaffe sig penge eller oplysninger.

Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste udsender jævnligt advarsler om forskellige typer af angreb og på deres hjemmeside finder man også en række vejledninger om, hvordan man kan sikre sig bedst muligt mod angreb.

12.3.1 Medarbejdere og adfærd

Mange angreb fra internettet starter med, at en medarbejder uforvarende foretager sig en handling på sin pc-arbejdsplads. Det kan være en bannerreklame på en webside, der bliver klikket på, et link eller en vedhæftet fil i en mail, der bliver åbnet.

Derfor er det vigtigt løbende at informere medarbejderne om informationssikkerhed, gennemføre awarenesskampagner og undervise medarbejderne i, hvordan de kan sikre sig mod at blive ofre for et hacker- eller virusangreb. Awarenesskampagner skal ligeledes bidrage til at medarbejderne har kendskab til gældende politikker og retningslinjer og dermed bidrager til at overholde gældende lovgivning i deres behandling af data og krav til fysisk sikkerhed.

12.3.1.2 Anvendelse af cloud-baseret løsninger

Internettet giver mange muligheder for at kommunikere med kolleger i andre organisationer og lande og der eksisterer efterhånden mange løsninger, hvor man kan dele informationer mellem forskellige organisationer, f.eks. i projektsammenhæng.

Hvis der anvendes produkter som Projectplace, Dropbox o.l. i forbindelse med et projekt, skal man være opmærksom på, at disse løsninger, giver anledning til en række udfordringer i forhold til persondatalovens krav til beskyttelse af personoplysninger.

Flere offentlige myndigheder er begyndt at anvende Cloud-baserede løsninger, f.eks. Microsoft 365. Ved anvendelse af en cloud-løsning, skal man sikre sig, at løsningen lever op til persondatalovens og sikkerhedsbekendtgørelsens krav, herunder at der er indgået en databehandleraftale og en EU-standardkontrakt, hvis der er tale om en leverandør i et usikkert tredjeland.

Som medarbejder i en offentlig myndighed må man i arbejdsmedfør kun anvende cloud løsninger som myndigheden har godkendt.

12.4 Sikker udvikling af it-løsninger

Ved udvikling eller anskaffelse af it-løsninger til sundhedsvæsenet er det vigtigt, at man får stillet de rigtige krav til informationssikkerhed.

I forhold til brugerstyring er det f.eks. vigtigt, at løsningerne kan leve op til de krav til differentiering og teknisk begrænsning af brugernes adgang, som kræves i lovgivningen og at man kan lave logopfølgning og efterforske, om der er brugere, der har misbrugt deres rettigheder.

Det kan også være forhold omkring håndtering af samtykke, værdispring eller overdragelse af en behandlingsrelation til en anden sundhedsperson, som det er relevant at få beskrevet krav for.

For organisationer, der udvikler eller anskaffer it-løsninger i henhold til en fastlagt projektmodel, anbefales det, at man eksplicit indføjer informationssikkerhed i de relevante projektfaser: ved projektstart, ved kravspecifikation og driftsoverdragelse.

12.41. Apps som medicinsk udstyr

Apps vurderes jf. EU-kommissionens direktiv som medicinsk udstyr på linje med ”stand-alone-software”.

Anvendelse af forskellige former for apps f.eks. til at opsamle helbredsoplysninger hos patienter eller til kommunikation mellem patient og behandler bliver mere udbredt, ikke mindst i relation til, at der etableres flere telemedicinske løsninger.

Hvis en app bliver brugt til at behandle og kommunikere personoplysninger, er det vigtigt at den lever op til persondatalovens og sikkerhedsbekendtgørelsens krav. Mange apps er udviklet til privates brug og der har ikke nødvendigvis været fokus på at gøre løsningen mindre sårbar over for trusler fra internettet. Inden en app tages i brug i en sundhedsfaglig sammenhæng, skal man derfor vurdere, om den kan leve op til sikkerhedskravene, f.eks. om der er etableret et MDM-system, der sikrer anvendelsen af appén

Lægemiddelstyrelsen har udgivet vejledninger til borgere og til leverandører, som beskriver, hvornår en app skal betragtes som medicinsk udstyr og dermed leve op til kravene i CE-mærkningsordningen. CE-mærkningen stiller ikke specifikke krav til informationssikkerhed, men hvis der er tale om medicinsk udstyr, følger det implicit.

Til brug for vurdering af, om en app skal betragtes som medicinsk udstyr eller ikke har Lægemiddelstyrelsen udarbejdet en beslutningsgraf, som er relevant at bruge både for leverandører, der laver apps, men også for sundhedspersoner, som anvender eller overvejer at anvende apps i patientbehandlingen.

12.4.2 Test

For at sikre, at nye versioner af en it-løsning fungerer og ikke kompromitterer hverken patientsikkerhed eller informationssikkerhed, er det vigtigt at der foretages test af alle ændringer, inden de bliver sat i produktion. Dette skal ske i et testmiljø, der ligner produktionsmiljøet så meget som muligt, så evt. fejl og mangler kan opdages og rettes, inden systemet flyttes til produktionsmiljøet.

Det er derfor vigtigt, at man i forbindelse med udvikling eller anskaffelse af en ny it-løsning får specificeret de relevante krav til et testmiljø. Hvis der er tale om mobile løsninger med apps til mobiltelefoner, tablets e.l., skal man sikre sig, at de testes med de operativsystemer, som tænkes anvendt (Android, Windows, IoS osv). Ligeledes bør man, inden systemer, der indeholder personoplysninger, tages i drift, foretage sårbarheds- og penetrationstests for at afklare evt. sikkerhedsrisici.

Mange eksisterende it-løsninger i sundhedsvæsenet har ikke tilknyttet testfaciliteter, og det kan derfor være vanskeligt at få testet nye versioner eller funktioner tilstrækkeligt, inden de placeres i produktionsmiljøet. Hvis man ikke har mulighed for at teste ændringer eller fejlrettelser, inden de implementeres i produktionssystemet, bør man meget hurtigt gennemføre tests, der kan verificere, om systemet fortsat fungerer korrekt.

Bilag 1 Litteraturliste

For så vidt angår referencer til love bemærkes det, at lovene og samtlige vedtagne lovændringer er tilgængelige på www.retsinformation.dk. Lovene findes ved at skrive lovens nr. og året for vedtagelsen i feltet øverst til venstre.

Apotekerloven (Bekendtgørelse af lov om apoteksvirksomhed), lovbekendtgørelse 1040 af 3. september 2014. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/Forms/r0710.aspx?id=164756.

Arkivloven (Bekendtgørelse af arkivloven), lovbekendtgørelse nr. 1035 af 21. august 2007. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/forms/r0710.aspx?id=12066.

Autorisationsloven (Bekendtgørelse af lov om autorisation af sundhedspersoner og om sundhedsfaglig virksomhed), lovbekendtgørelse nr. 877 af 4. august 2011. Lokaliseret d. 4. januar på https://www.retsinformation.dk/Forms/R0710.Aspx?id=138178.

Bekendtgørelse af lov om klage- og erstatningsadgang inden for sundhedsvæsenet, Lovbekendtgørelse nr. 1113 af 7. november 2013. Lokaliseret 6. april 2016 på

https://www.retsinformation.dk/forms/r0710.aspx?id=138893

Bekendtgørelse om autoriserede sundhedspersoners benyttelse af medhjælp (delegation af forbeholdt sundhedsfaglig virksomhed), bekendtgørelse nr. 1219 af 11. december 2009. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/Forms/R0710.aspx?id=129042.

Bekendtgørelse om godkendelse af landsdækkende og regionale kliniske kvalitetsdatabaser, bekendtgørelse nr. 851 af 2. juni 2015. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/Forms/R0710.aspx?id=173197&exp=1.

Bekendtgørelse om indberetning af oplysninger til kliniske kvalitetsdatabaser m.v., bekendtgørelse nr. 1725 af 21. december 2006. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/Forms/R0710.aspx?id=11046.

Bekendtgørelse om information og samtykke til deltagelse i sundhedsvidenskabelige forskningsprojekter samt om anmeldelse af og tilsyn med sundhedsvidenskabelige forskningsprojekter, bekendtgørelse nr. 1149 af 30. september 2013. Lokaliseret d. 5. april 2016 på

https://www.retsinformation.dk/forms/R0710.aspx?id=158259

Bekendtgørelse om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning, bekendtgørelse nr. 529 af 15. juni. 2000.

Lokaliseret d. 7. april 2016 på https://www.retsinformation.dk/Forms/R0710.aspx?id=843.

Bekendtgørelse om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for en privat dataansvarlig, bekendtgørelse nr. 534 af 15. juni 2000. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/Forms/R0710.aspx?id=848.

Epidemiloven (Bekendtgørelse af lov om foranstaltninger mod smitsomme og andre overførbare sygdomme), lovbekendtgørelse nr. 814 af 27. august 2009. Lokaliseret d. 7. april 2016 på https://www.retsinformation.dk/forms/r0710.aspx?id=126093.

Forsikringsaftaleloven (Bekendtgørelse af lov om forsikringsaftaler), lovbekendtgørelse nr. 1237 af 9. november 2015. Lokaliseret d. 8. april 2016 på https://www.retsinformation.dk/forms/r0710.aspx?id=143090.

Forvaltningsloven (Bekendtgørelse af forvaltningsloven), lovbekendtgørelse nr. 433 af 22. april 2014. Lokaliseret d. 7. april 2016 på https://www.retsinformation.dk/forms/r0710.aspx?id=161411.

Forældreansvarsloven (Bekendtgørelse af forældreansvarsloven), lovbekendtgørelse nr. 1820 af 23. december 2015. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/forms/R0710.aspx?id=173278.

Journalføringsbekendtgørelsen (Bekendtgørelse om autoriserede sundhedspersoners patientjournaler (journalføring, opbevaring, videregivelse og overdragelse mv.)), bekendtgørelse nr. 3 af 2. januar 2013. Lokaliseret d. 4. januar på https://www.retsinformation.dk/Forms/R0710.aspx?id=144978.

Komiteloven (Lov om videnskabsetisk behandling af sundhedsvidenskabelige forskningsprojekter), lov nr. 593 af 14. juni 2011. Lokaliseret 3. april 2016 på https://www.retsinformation.dk/forms/r0710.aspx?id=137674

Lægemiddelloven (Bekendtgørelse af lov om lægemidler), lovbekendtgørelse nr. 506 af 20. april 2013. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/Forms/r0710.aspx?id=146586.

Offentlighedsloven (Lov om offentlighed i forvaltningen), lov nr. 606 af 12. juni 2013. Lokaliseret d. 5. april 2016 på

https://www.retsinformation.dk/forms/r0710.aspx?id=152299.

Persondataloven (Lov om behandling af personoplysninger), lov nr. 429 af 31. maj 2000. Lokaliseret d. 4 januar 2016 på https://www.retsinformation.dk/Forms/R0710.Aspx?id=828.

Retsplejeloven (Bekendtgørelse af lov om rettens pleje), lovbekendtgørelse nr. 1255 af 16. november 2015. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/Forms/R0710.Aspx?id=172923.

Retssikkerhedsloven (Lov om retssikkerhed og administration på det sociale område) Lovbekendtgørelse nr. 1052 af 8. september 2015. Lokaliseret 6. april 2016 på https://www.retsinformation.dk/Forms/R0710.aspx?id=173199

Serviceloven (Bekendtgørelse af lov o social service), lovbekendtgørelse 1284 af 17. november 2015. Lokaliseret 18. januar 2016 på https://www.retsinformation.dk/Forms/R0710.aspx?id=175036.

Sikkerhedsbekendtgørelsen (Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning), bekendtgørelse nr. 528 af 15. juni 2000. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/forms/R0710.aspx?id=842.

Sundhedsloven (Bekendtgørelse af sundhedsloven), lovbekendtgørelse nr. 1202 af 24. november 2014. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/Forms/r0710.aspx?id=152710.

Vejledning til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, vejledning nr. 37 af 2. april 2001. Lokaliseret d. 4. januar 2016 på https://www.retsinformation.dk/Forms/R0710.aspx?id=1002. S. 37.

Øvrige

Center for Cybersikkerhed. *Forside.* Lokaliseret d. 8. april 2016 på https://fe-ddis.dk/CFCS/Pages/cfcs.aspx#.

Center for Cybersikkerhed (2015). *Ny sikkerhedsanbefaling: It-sikkerhed på rejsen.* Lokaliseret d. 4. januar 2016 på https://fe-ddis.dk/cfcs/nyheder/arkiv/2015/Pages/NysikkerhedsanbefalingIt-sikkerhedp%C3%A5rejsen.aspx.

Danske Regioner (2011/2014). *Retningslinjer for anmeldelse af forsker-initieret sundhedsforskning i regionerne til Datatilsynet.* Lokaliseret d. 30. januar 2016 på

http://www.regioner.dk/sundhed/forskning/retningslinjer+for+anmeldelse+af+forsker-initieret+sundhedsforskning+i+regionerne+til+datatilsynet

Danske Regioner (2015). *Kontrakt om det frie sygehus eller udvidet ret til behandling for patienter med somatiske og psykiske lidelser.* Lokaliseret d. 7. april 2016 på https://www.sundhed.dk/content/cms/51/61351_duf-kontrakt-pr-192015.pdf:

Datatilsynet (2008/2015a). *Anmeld ændring.* Lokaliseret d. 8. april 2016 på https://www.datatilsynet.dk/blanketter/anmeld-aendring/.

Datatilsynet (2008/2015b). *Binding Corporate Rules (BCR).* Lokaliseret d. 4. januar 2016 på http://www.datatilsynet.dk/erhverv/tredjelande/binding-corporate-rules-bcr/.

Datatilsynet (2012) *Behandling af personoplysninger i cloud-løsningen Office 365, brevdato: 06.06.12, journalnummer: 2011-082-0216.* Lokaliseret 18. januar 2016 på http://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/behandling-af-personoplysninger-i-cloud-loesningen-office-365/

Datatilsynet (2015/2016). *Forskning i regionerne.* Lokaliseret d. 7. april 2016 på https://www.datatilsynet.dk/offentlig/forskning/forskning-i-regionerne/.

Datatilsynet (2008/2015c). *Forskningsbiobanker.* Lokaliseret d. 8 april 2016 på https://www.datatilsynet.dk/erhverv/forskere-og-medicinalfirmaer/forskningsbiobanker/.

Datatilsynet (2008/2015d). *Fællesanmeldelser.* Lokaliseret d. 7. april. 2016 på https://www.datatilsynet.dk/offentlig/anmeldelse/faellesanmeldelser/.

Datatilsynet (2014). *It-sikkerhedstekst ST1.* Flere faktorer i login. Lokaliseret d. 8. april 2016 på https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Publikationer/ST1.pdf

Datatilsynet (2014). *It.sikkerhedstekst ST2.* Overvejelser om sikring mod, at personoplysninger kommer til uvedkommendes kendskab i forbindelse med datatransmission. Lokaliseret d. 8. april 2016 på https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Publikationer/ST2.pdf.

Datatilsynet (2014). *It-sikkerhedstekst ST4.* Datatransmission af personoplysninger på det åbne net. Lokaliseret d. 8. april 2016 på https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Publikationer/ST4.pdf.

Datatilsynet (2015). Kritik af Region Midtjyllands indberetning af fælles elektronisk patientjournal, brevdato 30.01.15, journalnummer: 2012-622-0004, 2014-632-0075 Lokaliseret d. 4. januar på http://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/vedroerende-region-midtjyllands-faelles-elektroniske-patientjournal-midtepj/.

Datatilsynet (2010). *Kritik til Erhvervs- og Selskabsstyrelsen for brud på persondataloven, brevdato: 28.09.10, journalnummer: 2009-621-0045.* Lokaliseret d. 8. april 2016 på https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/kritik-til-erhvervs-og-selskabsstyrelsen-for-brud-paa-persondataloven/.

Datatilsynet (2015/2015). *Ny procedure for anmeldelse af forskning og statistik.* Lokaliseret d. 7. april 2016 på https://www.datatilsynet.dk/offentlig/forskning/forskning-og-statistik-i-stat-og-kommuner/ny-procedure-for-anmeldelse-af-forskning-og-statistik/.

Datatilsynet (2007/2015). *Om anmeldelsessystemet.* Lokaliseret d. 8 april 2016 på https://www.datatilsynet.dk/blanketter/om-anmeldelsessystemet/.

Datatilsynet (2013/2015). *Sikre tredjelande.* Lokaliseret d. 4. januar 2016 på http://www.datatilsynet.dk/erhverv/tredjelande/sikre-tredjelande/.

Digitaliseringsstyrelsen (2015). *Guide til implementering af ISO27001.* Lokaliseret 21. maj 2016 på http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Implementering-af-ISO27001

Digitaliseringsstyrelsen (2015). *Informationssikkerhedspolitik.* Lokaliseret 18. januar 2016 på http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Vejledninger-om-sikkerhedsarbejdet/Informationssikkerhedspolitik. .

Digitaliseringsstyrelsen (2015). *Sikker e-mail – Om Nem-ID.* Lokaliseret d. 4. januar 2016 på https://www.nemid.nu/dk-da/om_nemid/hvad_er_nemid/sikker_e-mail/ .

Europa-kommissionen (2016). *Nyt værn om privatlivets fred: Europa-Kommissionen og USA når til enighed om en ny ordning for transatlantiske datastrømme.* Lokaliseret d. 8. april på http://europa.eu/rapid/press-release_IP-16-216_da.htm.

Europa-Parlamentet og Rådets direktiv 93/42EØF af 14. juni 1993, om medicinsk udstyr. Lokaliseret d. 8. april 2016 på http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:DA:PDF.

Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995, om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, artikel 8. Lokaliseret d. 4. januar 2016 på

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DA:HTML.

Indenrigs- og Sundhedsministeriet (2007). Oversigt over de juridiske rammer for adgangen til EPJ og IT-anvendelsen i sundhedsvæsenet.

Lægemiddelstyrelsen (2009/2016). *Vejledning til fabrikanter af medicinsk udstyr i klasse I.* Lokaliseret d. 8. april 2016 på http://laegemiddelstyrelsen.dk/da/udstyr/lovgivning-og-vejledning/sundhedsstyrelsens-vejledninger/vejledning-til-fabrikanter-af-medicinsk-udstyr-i-klasse-i#Hvorfor skal medicinsk udstyr CE-mærkes.

Lægemiddelstyrelsen (2015). *Beslutningsmodel for sundheds-apps og software.* Lokaliseret 4. januar 2016 på https://sundhedsstyrelsen.dk/da/medicin/medicinsk-udstyr/lovgivning-og-vejledning/sundhedsstyrelsens-vejledninger/~/media/53F2E52FB94C4BE495213EF0ED013A59.ashx.

MedCom (2015). *Infrastruktur.* Det danske sundhedsdatanet. Lokaliseret d. 4. januar 2016 på http://medcom.dk/wm110009.

Den Nationale Videnskabsetiske Komité (2014). *Fælles anmeldelse af kliniske forsøg med lægemidler.* Lokaliseret d. 4. januar 2016 på http://www.dnvk.dk/forskere/hvordansoegerjeg/Faelles%20anmeldelse.aspx.

Den Nationale Videnskabsetiske Komité (2016). *Retningslinjer for Komitésystemets behandling af sundhedsvidenskabelige forskningsprojekter med omfattende korlægning af individets arvemasse, version 5.* Lokaliseret d. 8 april 2016 på http://www.dnvk.dk/~/media/Files/cvk/forskere/Hvordan%20soeger%20jeg/Retningslinjer%20genom%20Version%205%20DOR10040S.ashx.

Sundhedsdatastyrelsen (2014). *Vejledning i adgang til registerdata hos Sundhedsdatastyrelsens Forskerservice,* udkast. Lokaliseret d. 8.april 2016 på http://sundhedsdatastyrelsen.dk/-/media/sds/filer/forskerservice/vejledning-forskerservice.pdf?la=da

Sundhedsdatastyrelsen (2016). *National Sundheds-It drfitsstatus.* Lokaliseret 4. januar 2016 på https://www.nspop.dk. .

Sundhedsstyrelsen (2011). *Smitsomme sygdomme med cpr-baseret anmeldepligt.* Lokaliseret d. 4. januar 2016 på https://sundhedsstyrelsen.dk/da/sundhed/smitsomme-sygdomme/~/media/056EABDB272945A38BBF13470C43A61F.ashx.

De Videnskabsetiske Komitéer (2008): Anmeldelse til de Videnskabsetiske Komitéer. Lokaliseret 18. januar 2016 på http://www.drvk.dk/anmeldelse/Anmeldelse.html.