Vejledning om informationssikkerhed

i

sundhedsvæsenet

HØRINGSVERSION

Indholdsfortegnelse

[1. Baggrund, formål og målgruppe 5](#_Toc442019676)

[1.2 Afgrænsninger 5](#_Toc442019677)

[1.3 Arbejdsgruppens sammensætning 6](#_Toc442019678)

[2. Læsevejledning 7](#_Toc442019679)

[3. Adgang til data – lovkrav 8](#_Toc442019680)

[3.1 Behandlingsøjemed 10](#_Toc442019681)

[3.1.1Journaliseringspligt og sundhedspersoners adgang til patientoplysninger 10](#_Toc442019682)

[*3.1.2.Videregivelse af oplysninger til behandlingsformål* 10](#_Toc442019683)

[3.1.3 Elektronisk indhentning af patientoplysninger 11](#_Toc442019684)

[3.1.4 Samtykke og retten til at frabede sig indhentning eller videregivelse 12](#_Toc442019685)

[3.1.5 Værdispringsreglen 13](#_Toc442019686)

[3.1.6 Beslutningsgraf vedr. sundhedspersoners indhentning af patientoplysninger 13](#_Toc442019687)

[3.2 Sekundær anvendelse 14](#_Toc442019688)

[3.2.1 Administration, herunder ledelsesinformation og afregning 15](#_Toc442019689)

[3.2.2 Kvalitetssikring mv. 16](#_Toc442019690)

[3.2.3 Videnskabelige og statistiske undersøgelser 16](#_Toc442019691)

[3.2.4 Andet 17](#_Toc442019692)

[4. Dataansvar 18](#_Toc442019693)

[4.1 Den dataansvarliges forpligtelser 18](#_Toc442019694)

[4.2 Hjemmel til behandling af oplysninger 19](#_Toc442019695)

[4.3 Databehandlere 20](#_Toc442019696)

[4.3.1 Indholdet af den skriftlige databehandleraftale 21](#_Toc442019697)

[4.4 Anmeldelse til datatilsynet. 21](#_Toc442019698)

[4.4.1 Den offentlige sektor 22](#_Toc442019699)

[4.4.2 Den private sektor 24](#_Toc442019700)

[4.4.3 Fællesanmeldelser 24](#_Toc442019701)

[4.4.4 Skabelon til anmeldelse 25](#_Toc442019702)

[4.4.5. Ændring af anmeldte behandlinger 25](#_Toc442019703)

[4.5 Overblik over dataflow 25](#_Toc442019704)

[Figur 4.1 Dataflowanalyse 1 26](#_Toc442019705)

[5. Deling af data på tværs af sektorer 27](#_Toc442019706)

[5.1 Hvordan deles data? 27](#_Toc442019707)

[5.2 Betingelser for deling af data på sundhedsområdet 28](#_Toc442019708)

[5.3 Landsdækkende databaser 30](#_Toc442019709)

[6. Adgang til borgerens data 31](#_Toc442019710)

[7. Borgerens adgang til oplysninger 32](#_Toc442019711)

[7.1 Aktindsigt og registerindsigt 32](#_Toc442019712)

[7.2 Adgang til egne sundhedsdata 32](#_Toc442019713)

[7.3 Adgang til logoplysninger 33](#_Toc442019714)

[7.4 Adgang til andres data 33](#_Toc442019715)

[7.4.1 Forældremyndighed eller værgemål 33](#_Toc442019716)

[7.4.2 Samtykke og fuldmagt 34](#_Toc442019717)

[7.4.3 Dødsfald 34](#_Toc442019718)

[7.4.4. Politi 35](#_Toc442019719)

[7.4.5 Andre 35](#_Toc442019720)

[8. Adgang til data til videnskabeligt eller statistisk formål 36](#_Toc442019721)

[8.1 Sundhedsvidenskabelig forskning på mennesker eller biologisk materiale 36](#_Toc442019722)

[8.2 Videregivelse af oplysninger fra patientjournaler 37](#_Toc442019723)

[8.3 Registerforskning 37](#_Toc442019724)

[8.4 Kvalitetsdatabaser 38](#_Toc442019725)

[8.5 Biobanker 39](#_Toc442019726)

[8.6 Videregivelse til andre forskningsprojekter 39](#_Toc442019727)

[8.7 Offentlig eller privat forskning 40](#_Toc442019728)

[8.8 Pseudonymisering, anonymisering og diskretionering 40](#_Toc442019729)

[8.8.1. Pseudonymisering 40](#_Toc442019730)

[8.8.2 Anonymisering 40](#_Toc442019731)

[*8.8.2.1* Diskretionering 40](#_Toc442019732)

[8.9 Big data 41](#_Toc442019733)

[9. Overførsel af patientoplysninger til EU- og tredjelande 42](#_Toc442019734)

[9.1 Overladelse til databehandlere 43](#_Toc442019735)

[9.2. Særligt vedr. videnskabelige og statistiske undersøgelser 43](#_Toc442019736)

[9.2 Beskyttelse af personoplysninger ved rejse i udlandet 43](#_Toc442019737)

[10. Netværkssikkerhed 44](#_Toc442019738)

[10.1 Intern kommunikation 44](#_Toc442019739)

[10.2 Ekstern kommunikation 44](#_Toc442019740)

[10.2.1 Det åbne internet 44](#_Toc442019741)

[10.2.2 Sundhedsdatanettet 45](#_Toc442019742)

[10.3 Den nationale serviceplatform 46](#_Toc442019743)

[11. Mobil sikkerhed 48](#_Toc442019744)

[11.1 Hvad er mobile enheder? 48](#_Toc442019745)

[11.2 Trusler 48](#_Toc442019746)

[11.3 Løsninger 48](#_Toc442019747)

[12. Krav vedr. informationssikkerhed 51](#_Toc442019748)

[12.1 Informationssikkerhed er mere end it-sikkerhed 51](#_Toc442019749)

[12.2 Anvendelse af standard for informationssikkerhed 51](#_Toc442019750)

[12.2.1. Ledelsesværktøj 52](#_Toc442019751)

[12.2.2. Risikovurdering 52](#_Toc442019752)

[12.3 Cybersikkerhed 52](#_Toc442019753)

[12.3.1 Medarbejdere og adfærd 52](#_Toc442019754)

[12.4 Sikker udvikling af it-løsninger 53](#_Toc442019755)

[12.41. Apps som medicinsk udstyr 53](#_Toc442019756)

[12.4.2 Test 54](#_Toc442019757)

[Bilag 1 Litteraturliste 55](#_Toc442019758)

# 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.

Vejledningen er ikke udtømmende i forhold til, hvordan man sikrer et tilstrækkeligt informationssikkerhedsniveau. Dels har vi valgt at henvise til andre – mere generelle - vejledninger, som er relevante også for sundhedsvæsenet, 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.

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.

## 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.

De ændringer, som følger af persondataforordningen, vil blive indarbejdet i næste version af vejledningen 2016.

## 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, departementet, 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)

# Læsevejledning

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

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

**Kapitel 3** omhandler de lovkrav, der fastlægger, under hvilke betingelser, forskellige faggrupper må få adgang til patientoplysninger. Kapitlet behandler adgang til data i forhold til de angivne formål for databehandlingen: Patientbehandling, kvalitetssikring, forskning m.v.

I **kapitel 4** beskrives det ansvar, der påhviler den dataansvarlige, herunder krav om anmeldelse til Datatilsynet og indgåelse af databehandleraftaler.

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, **kapitel** **6** beskriver forhold omkring adgang til borgernes egne data, mens **kapitel 7** omhandler borgernes adgang til deres egne oplysninger.

**Kapitel 8** går dybere ind i, under hvilke omstændigheder data må anvendes til videnskabelige formål, statistik og kvalitetssikring, mens **kapitel 9** omhandler beskyttelse af oplysninger 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 er best practice for den offentlige sektor.

# 3. Adgang til data – lovkrav

Adgangen til patientoplysninger er reguleret i flere love.

Det er først og fremmest sundhedsloven, der supplerer persondatalovens mere generelle bestemmelser,

[Sundhedsloven](https://www.retsinformation.dk/Forms/r0710.aspx?id=152710) regulerer bl.a. 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](https://www.retsinformation.dk/Forms/R0710.Aspx?id=828) er den lov, der implementerer EU's databeskyttelsesdirektiv i dansk lovgivning. Persondataloven anvendes, medmindre regler i anden lovgivning giver den registrerede en bedre retsstilling.

Persondatalovens §§ 6-8 indeholder generelle betingelser for, hvornår behandling af henholdsvis ikke-følsomme (herunder fortrolige) og følsomme oplysninger kan finde sted. Bestemmelser for sundhedsområdet findes i § 7, der bl.a. omhandler helbredsoplysninger.

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

Både persondatalovens og sundhedslovens bestemmelser skal være opfyldt. Det er sikret ved, at sundhedslovens bestemmelser er harmoniseret med persondataloven og at sundhedsloven langt hen ad vejen stiller borgeren bedre end persondataloven.

For det kommunale område er der ud over bestemmelserne i sundhedsloven og Persondataloven en række bestemmelser i [retssikkerhedsloven](https://www.retsinformation.dk/Forms/R0710.aspx?id=1834) og [serviceloven](https://www.retsinformation.dk/Forms/R0710.aspx?id=175036), der regulerer adgangen til personoplysninger.

I [forvaltningsloven](https://www.retsinformation.dk/forms/r0710.aspx?id=161411) finder man de generelle bestemmelser om offentligt ansattes tavshedspligt.

[Autorisationsloven](https://www.retsinformation.dk/forms/r0710.aspx?id=138178) beskriver de forpligtelser, en autoriseret sundhedsperson er underlagt, herunder journalføringspligten.

Desuden findes der bestemmelser i [lægemiddelloven](https://www.retsinformation.dk/Forms/r0710.aspx?id=146586) og [apotekerloven,](https://www.retsinformation.dk/Forms/r0710.aspx?id=164756) som regulerer adgangen til at indsamle og behandle lægemiddeloplysninger.

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.

Ved sundhedspersoner forstås både personer, der er sundhedsfagligt autoriserede til at varetage sundhedsfaglige opgaver og personer, der arbejder efter [delegation](https://www.retsinformation.dk/Forms/R0710.aspx?id=129042) fra en sundhedsperson. Man skal deltage aktivt i forbindelse med patientbehandlingen for at kunne defineres som sundhedsperson, dvs. at f.eks. elever og studerende i konkrete situationer kan fungere som sundhedspersoner. Men der kan også være tale om ingeniører, der har ansvaret for medikoteknisk udstyr eller lærere og pædagoger, der indgår i behandlingen på det børnepsykiatriske område. 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, kan de jf. sundhedslovens §42a, stk. 2 få adgang til de samme oplysninger, som den autoriserede sundhedsperson har adgang til.

## 3.1 Behandlingsøjemed

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

### 3.1.1Journaliseringspligt og sundhedspersoners adgang til patientoplysninger

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

I autorisationsloven og den tilhørende journalførings[bekendtgørelse](https://www.retsinformation.dk/Forms/R0710.aspx?id=144978) reguleres sundhedspersoners journalføringspligt. Det betyder, at der lovgivningsmæssigt stilles krav om, at autoriserede sundhedspersoner skal føre ordnede optegnelser vedr. patientens behandling, dvs. at de skal registrere alle oplysninger, der er relevante.

Journaliseringen 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.

#### 3.1.2.Videregivelse af oplysninger til behandlingsformål

Til brug for aktuelt behandling af patienten er det muligt for sundhedspersoner at videregive oplysninger til andre sundhedspersoner.

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

*Med videregivelse menes, at en sundhedsperson kan overlade oplysninger til andre sundhedspersoner om patientens helbredsforhold, øvrige rent private oplysninger og andre fortrolige oplysninger, når det er nødvendigt for den aktuelle behandling af patienten*

Ved videregivelsen skal det vurderes, om materialet indeholder oplysninger, der tydeligvis ikke er nødvendige for den aktuelle behandling. Disse oplysninger må ikke videregives.

Det er i visse tilfælde også tilladt at videregivelse 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,

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

Hvis patienten har været henvist til behandling på et privat sygehus eller klinik, hvor behandlingen er sket efter aftale med regionen eller kommunen, kan den læge, der har behandlet patienten på sygehuset eller klinikken ligeledes sende et udskrivningsbrev 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 denne.

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](https://sundhedsstyrelsen.dk/da/sundhed/smitsomme-sygdomme/~/media/056EABDB272945A38BBF13470C43A61F.ashx).

I servicelovens § 49a findes der bestemmelser om, at sygeplejersker, sundhedsplejersker, læger, tandlæger og tandplejere ansat i kommunen må videregive (udveksle) oplysninger med 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. Der er ikke lovhjemmel til at videresende konkrete oplysninger elektronisk eller på papir.

### 3.1.3 Elektronisk indhentning af patientoplysninger

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, indhente både historiske og aktuelle oplysninger om patienten på tværs af sektorer og behandlingsenheder. Med historiske oplysninger menes oplysninger, der ikke er indsamlet i forbindelse med den aktuelle behandling. Det kan altså godt være oplysninger fra et igangværende behandlingsforløb et andet sted i sundhedsvæsenet.

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

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.

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[[1]](#footnote-1).

Datatilsynet har da også i sin [afgørelse](http://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/vedroerende-region-midtjyllands-faelles-elektroniske-patientjournal-midtepj/) om adgang til patientjournaler i Region Midtjylland påtalt, at der er givet en meget bred adgang til patientoplysninger.

Loven giver mulighed for, at ledelsen på sygehuset 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.

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

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.

Der må også for disse grupper ske indhentning af dokumentation for kvalifikationer, de har erhvervet sig i et uddannelsesforløb, hvis der tages hensyn til patientens interesse og behov.

Indhentning skal ske umiddelbart 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.

Det anbefales, at man noterer formålet med indhentningen i patientens journal.

### 3.1.4 Samtykke og retten til at frabede sig indhentning eller videregivelse

I sundhedsloven er det angivet, at man med patientens samtykke kan videregive nødvendige oplysninger til andre sundhedspersoner, men at det kan ske uden patientens specifikke samtykke, hvis det drejer sig om et aktuelt behandlingsforløb, og der tages hensyn til patientens interesser og behov.

Forudsætningen er, at patienten er blevet gjort bekendt med, at han har mulighed for at frabede sig, at hans oplysninger videregives. Dette gælder også for elektronisk indhentning, hvor der ikke er krav om et specifikt samtykke fra patienten, når det drejer sig om indhentning af nødvendige oplysninger til et aktuelt behandlingsforløb.

Samtykke skal være udtrykkeligt og frivilligt, mundtligt eller skriftligt og skal gives i forbindelse med det aktuelle behov for videregivelse/indhentning

Samtykke til videregivelse eller oplysning om, at patienten har frabedt sig elektronisk indhentning skal dokumenteres i patientjournalen eller på anden måde. Det er vigtigt, at sundhedspersoner, der indgår i den aktuelle behandling, bliver gjort opmærksomme på, hvis en patient har frabedt sig videregivelse eller indhentning, så det skal tydeligt fremgå i skærmbilledet eller papirjournalen. Det skal også fremgå, at man har informeret patienten om konsekvenserne ved, at de frabeder sig videregivelse af oplysninger.

Da bevisbyrden for, at der foreligger et samtykke ligger hos myndigheden, anbefales det, at ma så vidt muligt indhenter et skriftligt samtykke fra patienten.

I retssikkerhedsloven, der gælder for det sociale område i kommunerne, er kravet om samtykke beskrevet i §11. 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.

### 3.1.5 Værdispringsreglen

Værdispringsreglens oprindelige grundlag findes i forvaltningslovens §28, stk. 2, nr. 3. Efter denne regel er en forvaltningsmyndighed berettiget til at give meget 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. I sundhedsloven findes der ligeledes værdispringsregler, f.eks. i § 42a, stk. 5, der siger, at værdispringsreglen kan anvendes ved 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 kunne hente oplysninger om et sammenligneligt tilfælde i behandling af sjældent forekommende, alvorlig sygdom. Her overstiger hensynet til den akutte 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 klare regler for dokumentation og opfølgning på anvendelsen.

### 3.1.6 Beslutningsgraf vedr. sundhedspersoners 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.

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

## Sekundær anvendelse

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

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.

Samtykke 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,
* videregivelsen er nødvendig for berettiget varetagelse af en åbenbar almen interesse eller af væsentlige hensyn til patienten, sundhedspersonen eller andre eller
* videregivelsen er nødvendig for, at en myndighed kan gennemføre tilsyns- og kontrolopgaver.

Videregivelse af patientoplysninger til andre formål end behandling uden patientens samtykke skal have hjemmel i lovgivningen.

### 3.2.1 Administration, herunder ledelsesinformation og afregning

For administrative formål, der kræver behandling af oplysninger på personniveau 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 har pligt til at videregive oplysningerne.

Af retssikkerhedsloven fremgår, at kommuner og sygehuse uden samtykke må udveksle oplysninger om indlæggelse og udskrivning af borgere i kommunen (advis).

Uden patientens samtykke kan oplysninger videregives til varetagelse af åbenbar almen interesse eller, hensyn til patienten selv eller som led i myndighedens tilsyns- og kontrolopgaver. Bestemmelsen skal fortolkes snævert og der skal være saglige grunde for at anvende bestemmelsen, f.eks. en pligt, som en myndighed er pålagt.

Som udgangspunkt må der ikke være personoplysninger i systemer til planlægning og ledelsesinformation.

Med ændringen af Sundhedsloven i 2011 fik kommuner og regioner adgang til eSundhed med henblik på planlægning og tilrettelæggelse af indsatsen på sundhedsområdet jf. § 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 ikke 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 oplysninger på individniveau vedr. sygehusbehandling, behandling i speciallægepraksis og behandling på private sygehuse og klinikker skal indberettes til Statens Seruminstitut med henblik på at dokumentere aktiviteten og danne grundlag for gruppering i DRG- eller DAGS-grupper, som anvendes til afregning mellem parterne.

*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.*

I forhold til praksissektorens afregning med sygesikringen 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.

### 3.2.2 Kvalitetssikring mv.

Efter sundhedslovens § 196 har ministeren 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](https://www.retsinformation.dk/Forms/R0710.aspx?id=11046) 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](https://www.retsinformation.dk/Forms/R0710.aspx?id=173197https://www.retsinformation.dk/Forms/R0710.aspx?id=173197) 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 på baggrund af § 43, stk. 2, pkt. 3 indhente de nødvendige oplysninger og videregive disse til den ansvarlige for kvalitetsdatabasen.

### 3.2.3 Videnskabelige og statistiske undersøgelser

Videregivelse til videnskabelige og statistiske formål er reguleret i sundhedslovens §46. Da sundhedsloven har adskilt indhentning og videregivelse, indebærer det, at det er den sundhedsperson, der har ansvaret for oplysningerne, der må videregive data til videnskabelige eller statistiske formål.

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

Den, der har ansvaret for de data, 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 delegation overdrages til en betroet medarbejder eller en sekretær, der yder teknisk bistand, under den pågældende sundhedspersons ansvar.

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

Udgangspunktet for at videregive data fra en patientjournal e.l. til videnskabelige eller statistiske formål er, at patientens samtykke indhentes. Samtykket skal journaliseres og bortfalder efter 1 år.

Såfremt det ikke er muligt eller meget uhensigtsmæssigt at indhente et samtykke fra patienten, kan data fra patientbehandlingssystemer videregives uden patientens samtykke til brug for et konkret sundhedsvidenskabeligt forskningsprojekt med udgangspunkt i sundhedslovens § 46, såfremt der er indhentet tilladelse til projektet fra enten en videnskabsetisk komité eller Sundhedsstyrelsen. Hvis projektet ikke er omfattet af reglerne for Videnskabsetisk komité, skal Sundhedsstyrelsen give tilladelse til videregivelse af data til det konkret forskningsprojekt. I nogle tilfælde kræver den videnskabsetiske komité, at der også foreligger en godkendelse fra Sundhedsstyrelsen.

Der kræves i henhold til persondataloven ikke patientens samtykke, når følsomme persondata anvendes til statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, jf. persondatalovens § 10, stk. 1.

Oplysninger fra videnskabelige og statistiske undersøgelser må ikke offentliggøres på individniveau.

### 3.2.4 Andet

Patienternes oplysning kan videregives til andre formål, men det kræver altid patientens skriftlige samtykke, hvis der ikke er tale om, at videregivelsen sker på baggrund af et lovkrav, åbenbar almen interesse eller væsentlige hensyn til patienten eller andre eller som led i myndighedens tilsyns- og kontrolopgaver.

Det kræver således et konkret informeret 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.

# Dataansvar

Persondataloven beskriver, hvordan man må behandle 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, formidling, sammenstilling, samkøring, blokering og sletning – uanset om det foregår digitalt eller manuelt.

Persondataloven opererer med to roller: den dataansvarlige og databehandleren. Den dataansvarlige er den person eller myndighed, som har ansvaret for data og bestemmer, hvordan data må anvendes. Databehandleren behandler data på vegne af den dataansvarlige.

## 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 persondata. Det indebærer bl.a., at det er den dataansvarlige, der har pligt til at anmelde databehandlingen til Datatilsynet, når det er påkrævet (se afsnit 4.4), sikre, at borgerens rettigheder tilgodeses og som har ansvaret for, at der etableres de fornødne tekniske og organisatoriske sikringsforanstaltninger.

*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*

Disse sikringsforanstaltninger skal bidrage til, at oplysningerne ikke hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, at oplysningerne ikke kommer til uvedkommendes kendskab eller misbruges, eller at oplysningerne ikke behandles i strid med lov om behandling af 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, de er pålagt. Men det kan også være en praktiserende læge, der behandler patientoplysninger i forbindelse med sin praksis m.v. eller en sundhedsperson, der 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 [sikkerhedsbekendtgørelse](https://www.retsinformation.dk/forms/R0710.aspx?id=842)n. Sikkerhedsbekendtgørelsen indeholder bestemmelser om, hvilke sikringstiltag, der skal etableres, når der behandles persondata. Det kan f.eks. være brugeradministrationssystemer, som regulerer adgangen til data, retningslinjer for, hvem der må få adgang til bestemte persondata eller krav om logning af, hvem der har haft adgang til hvilke oplysninger.

For private virksomheder, herunder privatklinikker og privatpraktiserende læger er der ikke krav om at efterleve sikkerhedsbekendtgørelsens bestemmelser, men som det fremgår af [vejledningen](https://www.retsinformation.dk/Forms/R0710.aspx?id=1002) til sikkerhedsbekendtgørelsen, gælder persondatalovens bestemmelser umiddelbart. Datatilsynet anbefaler dog, at private aktører efterlever sikkerhedsbekendtgørelsens bestemmelser.

Eftersom der ikke er lovmæssigt krav til private sundhedsorganisationer 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**.**

For nogle databehandlinger, f.eks Sundhedsjournalen på sundhed.dk eller Mikrobiologidatabanken, er de enkelte regioner dataansvarlige for egne data, selv om de ligger i en fælles database.

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 anvende oplysningerne til andre formål end dem, de er indsamlet til.

Data kan videregives til andre dataansvarlige, hvis det er lovpligtigt eller hvis formålet med behandlingen hos den nye dataansvarlige ikke er 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 slettes eller blokeres.

## 4.2 Hjemmel til behandling af oplysninger

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

Hjemmel til indsamling og registrering i sundhedsvæsenet 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 (§1 og § 2).

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 (§3).

Herudover er der specifikke hjemmelsbestemmelser for det fælles medicinkort (FMK) og det danske vaccinationsregister (DDV) §157 og §157a, det nationale patientindeks i §193b, landsdækkende og regionale kliniske kvalitetsdatabaser i §196 og planlægning af indsatsen på sundhedsområdet §197.

Det fremgår af § 157, 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), ligesom de efter §157a er er ansvarlige for at drive en elektronisk registrering af oplysninger om de enkelte borgeres vaccinationer (DDV).

I § 193b bemyndigesministeren 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 loven gælder i modsætning til § 157 og §157a ikke en konkret eksisterende løsning.

Det fremgår af § 196, at Sundhedsdatastyrelsen godkender landsdækkende og regionale kliniske kvalitetsdatabaser, som en offentlig myndighed er dataansvarlig for. Sundhedsdatastyrelsen fastsætter nærmere [regler](https://www.retsinformation.dk/Forms/R0710.aspx?id=173197&exp=1) for procedure og kriterier for godkendelse af kliniske kvalitetsdatabaser og for kvalitetsdatabasernes virke.

Af § 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 § 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 patientombuddet (§ 199).

I forbindelse med registerforskning (defineret som videnskabelige eller statistiske undersøgelser, der alene bygger på data fra landsdækkende registre eller andre registre, der ikke er patientbehandlingssystemer) findes hjemmelen til databehandling ikke i sundhedsloven, men i persondatalovens §10.

## 4.3 Databehandlere

En dataansvarlig kan vælge at overlade det til en anden at udføre selve den praktiske behandling af personoplysninger på den dataansvarliges vegne, jf. afsnit 5.1., som betegnes som databehandler.

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, der behandler oplysninger på vegne af den dataansvarlige*

I praksis kan en databehandler være en virksomhed, som drifter en anden virksomheds eller en offentlig myndigheds IT-systemer. På sundhedsområdet fungerer MedCom f.eks. som databehandler for sundhedsvæsenets parter i forbindelse med drift af Sundhedsdatanettet, sundhed.dk, der er databehandler i forhold til en lang række tjenester, f.eks. Sundhedsjournalen og en række private leverandører, f.eks. CGI, der drifter Landspatientregisteret for Sundhedsdatastyrelsen.

En databehandler kan også være en leverandør, der alene har adgang til data 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 i forhold til den enkelte databehandling, 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 og det vil 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.

* + 1. Indholdet af den skriftlige databehandleraftale

Den skriftlige aftale imellem den dataansvarlige og databehandleren skal som minimum 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 indhente en årlig revisionserklæring fra en uafhængig tredjepart og databehandleraftalen bør indeholde krav om adgang til revisionserklæringen som en betingelse for at lade behandlingen foretage hos databehandleren.

Man skal være opmærksom på, at der også skal udarbejdes databehandleraftaler for medikoteknisk udstyr, såfremt der i tilknytning til udstyret findes en database, der indeholder patientoplysninger.

Som bilag til aftalen 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
* Logning
* Logopfølgning/audit
* Kryptering
* Håndtering af uddatamateriale
* Rekvirering af auditlog
* Procedure for 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.

## 4.4 Anmeldelse til datatilsynet.

Al databehandling af fortrolige og følsomme personoplysninger skal anmeldes til Datatilsynet. Formålet er at kunne kontrollere, at databehandlingen lever op til reglerne i Persondataloven.

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

Datatilsynet har indgået aftaler med en række offentlige myndigheder om, at man i stedet for at anmelde alle databehandlinger direkte til Datatilsynet, opererer med såkaldte paraplyanmeldelser, se afsnit 4.4.1.1.

### 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](https://www.retsinformation.dk/Forms/R0710.aspx?id=843) om undtagelse fra pligten til anmeldelse af visse behandlinger, som foretages for den offentlige forvaltning, er undtaget fra anmeldelsespligten – f.eks. personaleadministrations- og undervisningssystemer.

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

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

* 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
* 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.

For større fællesoffentlige systemer bør det vurderes konkret, hvorvidt behandlingen af personoplysninger tilsiger, at der skal indhentes en forudgående udtalelse fra Datatilsynet.

#### 4.4.1.1 Paraplyanmeldelser

For at forenkle anmeldelsesproceduren har regionerne og Datatilsynet i fællesskab udarbejdet et antal såkaldte **paraplyanmeldelser**, der omfatter regionernes behandlinger på sundhedsområdet.

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 til Datatilsynet.

Regionernes kontaktpersoner kan findes på Datatilsynets hjemmeside.

Hvis en databehandling kræver forudgående godkendelse af Datatilsynet, er det den regionale kontaktperson, der indhenter godkendelsen.

#### 4.4.1.2 Anmeldelse af behandling i videnskabeligt eller statistisk øjemed

I regionerne er der udarbejdet to paraplyanmeldelser, der samlet skal dække den forskning og kvalitetssikring på sundhedsområdet, der foregår i regionernes regi.

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. 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 – 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. Anmeldelserne opdateres løbende med nye databaser.

Regionernes anmeldelser findes på Datatilsynets hjemmeside.

4.4.1.3 Brug regionens kontaktperson

Som det fremgår, skal der ikke ske anmeldelse til Datatilsynet af hvert enkelt projekt eller database. De hospitaler, afdelinger eller forskere, der laver videnskabelige eller statistiske undersøgelser på regionernes ansvar, skal derfor ikke selv anmelde noget til Datatilsynet, men skal i stedet henvende sig til regionens kontaktperson, inden behandlingen af personoplysninger i forbindelse med undersøgelsen iværksættes.

4.4.1.4 Anmeldelser af ph.d.-projekter

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

### 4.4.2 Den private sektor

I den private del af sundhedssektoren skal der ligeledes foretages anmeldelse af behandling af fortrolige og følsomme oplysninger.

Som for den offentlige sektor er der en [undtagelsesbekendtgørelse](https://www.retsinformation.dk/forms/R0710.aspx?id=848) 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
* 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

Også i den private sektor skal der i en række tilfælde ikke alene foretages anmeldelse, men tillige indhentes forudgående udtalelse fra Datatilsynet. Dette er tilfældet, hvis behandlingen omfatter følsomme oplysninger (§7-8).

*Private skal ikke anmelde databehandling, der sker i behandlingsøjemed*

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

### 4.4.3 Fællesanmeldelser

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 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 KLs koordinator, 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.

### 4.4.4 Skabelon til anmeldelse

Anmeldelse til Datatilsynet af paraplyanmeldelser, fællesanmeldelser og private sker via deres hjemmeside, hvor der findes en [skabelon](http://www.datatilsynet.dk/blanketter/offentlig-sektor/blanket-til-oevrig-offentlig-virksomhed/blanket-til-oevrige-offentlige-anmeldelser/), der skal anvendes.

### 4.4.5. Ændring af anmeldte behandlinger

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 via KLs koordinator, 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 § 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.

## 4.5 Overblik over dataflow

Den dataansvarlige har ansvaret for at vide, hvor og hvordan de oplysninger, de har ansvaret for, behandles. Der bør derfor foretages en selvstændig kortlægning af datas livscyklus og vandring mellem den dataansvarlige, databehandlere og eventuelle tredjeparter, i form af en dataflowanalyse. Dataflowanalysen skal 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 bør 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 data end formålet tilsiger?
7. Sikres det, at data ikke anvendes til andre formål?
8. Sletningsregler for evt. midlertidige kopier af datasættet
9. Kortlægge hvilken behandling af data, der finder sted
10. Bestemme hvem der har adgang til personoplysninger
11. Bestemme hvem der er ansvarlig for datas sikkerhed
12. Hvordan organiseres personoplysningerne?
13. Videregives data til andre?
14. Slettes data, når behandlingsformålet ophører?

Beskrivelsen bør 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 1

# 5. Deling af data på tværs af sektorer

Med udgangspunkt i de lovgivningsmæssige rammer, som blev beskrevet i kapitel 4, beskrives i dette kapitel, under hvilke betingelser, der kan ske deling af data på tværs af sundhedssektoren, dvs. mellem f.eks. Social & Handicap, Ældre & Sundhed i kommunerne, sygehuse og praktiserende læger samt forslag til, hvordan man kan aftale og dokumentere datadeling, så det er i overensstemmelse med lovkravene.

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.

Deling af data bliver ofte brugt til at udtrykke, at oplysningerne skal kunne bruges af forskellige sundhedspersoner i deres behandling af patienten. I lovgivningsmæssig forstand er der tale om **videregivelse** eller **indhentning** af oplysninger, jf. kapitel 4.

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 data til rådighed for sundhedsvæsenets parter. Sundhedsdatastyrelsen driver det Fælles Medicinkort og regionerne udstiller via sundhed.dk Sundhedsjournalen.

## 5.1 Hvordan deles data?

Deling af data 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 deles ved at de placeres i et fælles datalager, når der er hjemmel hertil, som det f.eks. sker i det Fælles Medicinkort. Her kan en sundhedsperson, som har en aktuel behandlingsrelation, få adgang til oplysningerne, når det er nødvendigt.

Endelig må det antages, at der foregår en del kommunikation mellem parterne via elektronisk post, selv om det er svært at opgøre omfanget. I den offentlige sektor er det et krav, at der anvendes sikker post.

## 5.2 Betingelser for deling af data på sundhedsområdet

Som udgangspunkt skal den dataansvarlige sikre sig, at der er hjemmel i lovgivningen til at indsamle og videregive oplysningerne til andre parter i sundhedsvæsenet. I dette afsnit forudsættes, at data er lovligt indhentet, og afsnittet beskriver derfor alene betingelser for videregivelse og elektronisk indhentning.

Det er ikke sundhedspersonens organisatoriske placering, men deres rolle i forbindelse med patientbehandlingen, der er afgørende for, om de må få adgang til oplysninger eller ej, og data kan deles på tværs af sundhedsvæsenet, så længe reglerne i kapitel 9 overholdes.

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

I tværsektorielle projekter, hvor der skal ske deling af data, er det væsentligt, at der indledningsvist tages stilling til, hvem der dataansvarlig for data og dermed sætter rammerne for anvendelsen af data.

Den dataansvarlige for oplysningerne skal beskrive formålet med at data deles, f.eks. i dataanmeldelsen til Datatilsynet/paraplyanmeldelsen, så begrundelsen for, at bestemte faggrupper eller organisationer skal have adgang til data, er så konkret, at det fremgår, at oplysningerne er nødvendige for patientbehandlingen.

Den eller de dataansvarlige skal 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 data skal deles mellem f.eks. personale i kommunen og på sygehuset, gennemgå 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 beskriver rammerne for dataanvendelsen.
* Er der hjemmel i lovgivningen til deling af oplysningerne? Hvis der ikke er hjemmel, skal man sikre sig patientens samtykke, inden data må videregives eller indhentes

Hvis formålet ikke er omfattet af den eksisterende anmeldelse, skal der anmeldes en ændring til Datatilsynet (se kap. 4.4), som de skal godkende. Hvis der er tale om et helt nyt formål, skal der sandsynligvis laves en ny anmeldelse og man må kun dele data, 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.

Eftersom en sundhedsperson kun skal have adgang til de oplysninger, der er nødvendige for udførelsen af deres opgaver, er der forskel på, hvilke oplysninger f.eks. fra en elektronisk patientjournal, der er relevante for det personale i Social & Handicap, Ældre & Sundhed i kommunerne, som skal modtage en patient efter et sygehusophold og sikre, at de rigtige ydelser stilles til rådighed.

For de i sundhedslovens § 42a, stk. 2, nævnte sundhedspersoner[[2]](#footnote-2) 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.

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

* Dataansvarlig(e)
* Databehandlere
* Andre deltagere (dataanvendere)
* Formål med datadeling
* 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 data mellem sygehuse, der deltager i den aktuelle patientbehandling eller udsendelse af epikrise til egen læge efter sygehusophold, direkte i sundhedsloven eller bekendtgørelser i forhold til sundhedsloven.

Hvis man vil indgå en aftale om deling af data 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.

Den dataansvarlige skal dog altid have styr på dataflowet (se kap. 4.5), dvs. hvor de data, vedkommende har ansvaret for, flyder hen eller hvem, der har adgang til data.

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 data, hvis de f.eks. bliver vist som en integreret del af et it-system. Det gælder både i forhold til at sikre sig, at data 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 data 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 som udgangspunkt er en dataansvarlig, som sikrer, at data anvendes i henhold til formål og lovhjemmel.

Eksempler på sådanne landsdækkende databaser er det Fælles Medicinkort (§157), det Danske Vaccinationsregister (§157a) og det Nationale Patientindeks (§193b).

# 6. Adgang til borgerens data

I dag registreres der ikke kun helbredsoplysninger om borgerne i forbindelse med behandling i sundhedsvæsenet, men mange mennesker begynder at opsamle oplysninger om deres helbred i apps på deres mobiltelefon, i Microsoft HealthVault o.l.

Man skal derfor skelne 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 persondataloven eller sundhedsloven.

Sundhedspersoner er derfor som udgangspunkt ikke forpligtet til at forholde sig til de data, 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 registrerer data i et sundheds-it system, f.eks. en elektronisk omsorgsjournal, patientjournal eller et lægepraksissystem. Hvis data overføres eller registreres i et sundheds-it system, gælder de almindelige regler i sundhedsloven og retssikkerhedsloven m.v.

# Borgerens adgang til oplysninger

## 7.1 Aktindsigt og registerindsigt

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.

En patient, der er blevet undersøgt eller behandlet på et sygehus eller et andet behandlingssted har krav på at få aktindsigt 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.

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.

I henhold til Persondataloven har borgeren ret til indsigt i de oplysninger, der er registreret om vedkommende. 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 svare inden 4 uger efter modtagelse af anmodningen, og hvis dette ikke kan lade sig gøre, skal borgeren informeres om årsagen hertil.

Adgangen til indsigt gælder ikke for oplysninger, der udelukkende bruges til statistik og forskning, lige som den ikke gælder for logoplysninger, der primært anvendes til interne administrative formål.

## 7.2 Adgang til egne sundhedsdata

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

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 FMK og sundhedsjournalen fremgår, hvem der har foretaget opslag på patientdata.

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 data, 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.

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 man 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.

## 7.4 Adgang til andres data

### 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.

Selv om man ikke er indehaver af forældremyndigheden, har man som forældre lov til at blive orienteret om barnets helbred, jf. [forældreansvarsloven](https://www.retsinformation.dk/forms/R0710.aspx?id=173278)s §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.

Adgang til data 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 i sundhedsvæsenet udfyldes der 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 det.

Ifølge forvaltningslovens § 9 kan der kun gives aktindsigt til en pårørende, hvis der findes en fuldmagt fra borgeren. Hvis flere pårørende ønsker aktindsigt, skal de have individuelle fuldmagter.

Selv om en borger er dement, skal vedkommende selv frivilligt underskrive en fuldmagtserklæring. For at undgå, at der opstår tvivl om frivilligheden, anbefales det, at underskrift på fuldmagten overværes og skriftligt bevidnes af uafhængige vidner.

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, f.eks. ved underskrift på forsikringsansøgningen. Hvis journalen indeholder oplysninger, der ikke er relevante for forsikringsselskabet, skal disse udelades.

### 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. 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.

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](http://stps.dk/da/afgoerelser/afgoerelserfrapatientombuddet/patientrettigheder) i 2015 har klageren fået ret i, at samtykket burde gælde, også efter en længere periode.

Reglerne om aktindsigt gælder ikke for obduktionserklæringer, idet disse ikke danner grundlag for behandling af patienten.

### Politi

Politiets adgang til oplysninger om den enkelte er reguleret i [retsplejelovens](https://www.retsinformation.dk/Forms/R0710.Aspx?id=172923) kapitel 74 om beslaglæggelse og edition. Politiet må herefter som udgangspunkt kun få adgang til borgeres helbredsoplysninger, såfremt der foreligger en dommerkendelse. Hvis der er tale om grov kriminalitet og politiet anser det for nødvendigt at foretage en ”beslaglæggelse”, kan man kræve, at dette bliver prøvet for en domstol inden for 24 timer.

### Andre

Jf. offentlighedsloven kan journalister og andre kræve adgang til oplysninger hos offentlige myndigheder. Denne indsigt gælder ikke personoplysninger af fortrolig eller følsom karakter, der er registreret i databaser, som er omfattet af persondatalovens krav.

# Adgang til data 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, forskning i nye behandlingsmetoder, statistik m.m. Både sundhedsloven og persondataloven indeholder krav til, hvordan personoplysninger skal behandles og beskyttes i denne sammenhæng, jf. 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 den nationale videnskabsetiske komite eller en af de regionale videnskabsetiske komiteer ved at anvende komitesystemets [anmeldelsesportal](http://www.drvk.dk/anmeldelse/Anmeldelse.html) eller hvis der er tale om kliniske lægemiddelforsøg på Lægemiddelstyrelsens [portal](http://www.dnvk.dk/forskere/hvordansoegerjeg/Faelles%20anmeldelse.aspx).

I forhold til de data, 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 fuldt anonymiserede data.

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.

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

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

Data skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til personoplysninger. Kravene er beskrevet i [sikkerhedsbekendtgørelsen](https://www.retsinformation.dk/forms/r0710.aspx?id=842) og uddybes i den [vejledning til sikkerhedsbekendtgørelsen](https://www.retsinformation.dk/Forms/R0710.aspx?id=1002), som man også kan finde på Datatilsynets hjemmeside. Her kan man finde de konkrete krav til adgangsstyring, fysisk sikkerhed, logning m.v.

Hvis det er nødvendigt at opbevare data lokalt på en pc i kortere eller længere tid, skal oplysningerne krypteres. 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. F.eks. at ens database ikke åbner mulighed for, at man kan tilgå data uden om adgangsstyringssystemet og at man kan logge alle transaktioner, der foretages i databasen. Mange af de værktøjer, der stilles til rådighed, f.eks. Excel og Access, opfylder ikke disse krav.

Hos mange offentlige myndigheder er der fastlagt retningslinjer for, hvordan data skal opbevares og behandles. Man skal derfor inden projektets igangsættelse sikre sig, at man overholder retningslinjerne hos den pågældende myndighed.

Hvis man indsamler oplysninger hos de patienter, der indgår i projektet, skal de orienteres om formålet med projektet og hvem, der behandler oplysningerne og evt. andre modtagere af oplysningerne. Projektdeltagerne skal orienteres om, at det er frivilligt at deltage.

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

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

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](https://www.retsinformation.dk/forms/r0710.aspx?id=12066) regler.

Ved offentliggørelse af resultater fra projektet må man ikke kunne identificere enkeltpersoner (se nedenfor om diskretionering).

Overførsel af oplysninger til tredjelande eller anvendelse af databehandler i et tredjeland er behandlet i kapitel 12.

## 8.2 Videregivelse af oplysninger fra 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 administrerende overlæge på 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 rigtig mange oplysninger om patienter og deres behandling, som findes i en række statslige registre, som for nogens vedkommende har eksisteret i rigtig 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 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 administrative registre og ofte indgår der oplysninger fra flere registre i sådanne studier.

[Forskerservice](http://www.ssi.dk/~/media/Indhold/DK%20-%20dansk/Sundhedsdata%20og%20it/NSF/Forskerservice/Vejledning%20Forskerservice.ashx) 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 baserer sig på Persondatalovens bestemmelser.

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. Af hensyn til datasikkerheden udleveres der kun CPR-numre, hvis der eksplicit er behov herfor.

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.

## 8.4 Kvalitetsdatabaser

Kvalitetssikring er defineret som planlagte og systematiske aktiviteter, der skal sikre, at krav til kvalitet af et produkt eller en ydelse opfyldes.

En klinisk kvalitetsdatabase er et register, der indeholder data på målbare indikatorer, der tager udgangspunkt i det enkelte patientforløb. Databaserne bruges til at måle kvaliteten af den sundhedsfaglige behandling.

Landsdækkende og regionale kvalitetsdatabaser skal godkendes af Sundhedsdatastyrelsen, inden indsamling af data må igangsættes. Data fra kvalitetsdatabaserne må anvendes til kvalitetssikring i forhold til de indikatorer, der er opsat for den enkelte database. Data fra kliniske kvalitetsdatabaser må videregives til videnskabelige eller statistiske formål efter de gældende regler.

Ud over de godkendte kliniske kvalitetsdatabaser, som har hjemmel i sundhedslovens §196. er mulighederne for at indsamle helbredsoplysninger fra patientbehandlingssystemer til kvalitetssikringsformål begrænsede, med mindre der foreligger et samtykke fra patienten, som skal fornys årligt.

I nogle tilfælde kan der med hjemmel i sundhedslovens §43, stk. 2 nr. 3 om kontrol og tilsyn videregives helbredsoplysninger til sådanne databaser uden patientens samtykke. Det forudsætter, at registreringen er afgrænset til en enkelt afdeling og at der foreligger særlige hændelser forud, som f.eks. usædvanligt mange dødsfald eller mange tilfælde af multiresistente bakterier.

Denne type af kvalitetsdatabaser skal anmeldes og godkendes af Datatilsynet jf. §10, stk. 1. For regionerne hører den type af kliniske kvalitetsdatabaser under paraplyanmeldelsen for forskning.

Andre databaser, der skal bruges til kvalitetssikring, kan anmeldes med videnskabeligt eller statistisk formål i henhold til persondatalovens §7, stk. 5, såfremt man kan godtgøre, at det lever op til paragraffens bestemmelser om væsentlig samfundsmæssig nytte.

Personoplysninger må, som for andre videnskabelige eller statistiske undersøgelser, ikke efterfølgende anvendes i den direkte patientbehandling.

På behandlingssteder, hvor man har et kvalitetsmonitoreringsprogram, er de kvalitetsoplysninger, der indsamles og anvendes i forbindelse med den konkrete patientbehandling og registreres i patientjournalen at betragte som en del af registreringen i forbindelse med patientbehandlingen og behøver derfor ikke anmeldes særskilt.

## 8.5 Biobanker

En biobank er en samling af menneskeligt biologisk materiale, som indeholder oplysninger, der kan føres tilbage 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](http://www.datatilsynet.dk/erhverv/forskere-og-medicinalfirmaer/forskningsbiobanker/#c720), men projektet skal ikke anmeldes til Datatilsynet. Hvis der er tale om en offentlig myndighed, der er dataansvarlig, anmeldes biobanken i relation til det konkrete projekt.

For biobanker, 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 en selvstændig anmeldelse til Datatilsynet eller det skal fremgå af paraplyanmeldelsen vedr. forskning. Et eksempel herpå 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 ikke-personhenførbart 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 personhenførbart, skal der træffes særlige sikkerhedsforanstaltninger.

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

## 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. inkludering af en ny patientgruppe, 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.

Hvis den samme dataansvarlige vil anvende data fra et eksisterende forskningsprojekt i et nyt projekt inden for den dataansvarliges ansvarsområde, er der tale om overladelse 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 selvstændigt til Datatilsynet forinden, for regionerne sker dette under paraplyanmeldelsen for videnskabelig forskning.

Datatilsynet har den 12. juni 2015 meddelt regionerne generelle tilladelser til at videregive oplysninger omfattet af regionernes paraplyanmeldelser vedrørende sundhedsvidenskabelig forskning og kliniske kvalitetsdatabaser, der er godkendt af Sundhedsdatastyrelsen. 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 regionens 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, anonymisering og diskretionering

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 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 selv ikke personen, oplysningerne vedrører, vil være i stand til at genkende sig selv.

### 8.8.2.1 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 eller trunkering, hvor man grupperer værdierne på et niveau, der umuliggør genkendelse. 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.

Forudsætningen for, at oplysninger, der oprindeligt var personhenførbare, kan indgå i Big Data, er at data er fuldt anonymiserede.

Er det ikke muligt at anonymisere personoplysninger fuldstændigt. Gælder persondatalovens regler om, at data kun må indsamles og behandles i det omfang, det er nødvendigt og til det formål, som man i forbindelse med en videnskabelig eller statistisk undersøgelse, har anmeldt til Datatilsynet.

# 9. Overførsel af patientoplysninger til EU- og tredjelande

Persondataloven er implementeringen af [EU's persondatadirektiv](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:da:HTMLhttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:da:HTML) i dansk lov. Persondatadirektivet skal på den ene side skal beskytte de borgere, hvis oplysninger bliver behandlet og på den anden side sikre fri udveksling af sådanne oplysninger inden for EU.

Persondata 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 er overholdt. Det vil sige, at hvis det drejersig 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.

Tredjelande, som har indført en persondatalovgivning, der svarer til persondatadirektivet kan godkendes som sikre tredjelande. Det gælder for eksempel for Færøerne og Schweiz. EU-Kommissionen vurderer, at de lande, der er godkendt som [sikre tredjelande](http://www.datatilsynet.dk/erhverv/tredjelande/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 private dataansvarlige skal indhente en tilladelse.

Offentlige myndigheder skal, såfremt der er tale om en databehandler i et sikkert tredjeland, indgå en databehandleraftale med denne. Hvis der er tale om videregivelse til en anden dataansvarlig, skal dette fremgå af anmeldelsen til Datatilsynet.

For de lande, som af EU opfattes som usikre 3. lande, dvs. lande, der ikke har en persondatalov, der svarer til persondatadirektivet, skal man anvende [EU's standardkontrakt](http://www.datatilsynet.dk/erhverv/tredjelande/kommissionens-standardkontrakter/) til at fastlægge kravene i forhold til den organisation eller virksomhed, man vil overføre data til. Usikre tredjelande er f.eks. USA og Grønland.

Når man anvender EU’s standardkontrakt er det vigtigt, at der ikke ændres i kontraktens ordlyd. Hvis der ændres i kontraktens ordlyd, skal den godkendes af Datatilsynet, inden data kan overføres til tredjelandet.

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](http://www.datatilsynet.dk/erhverv/tredjelande/binding-corporate-rules-bcr/). 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. en EU-standardaftale som beskrevet ovenfor.

## 9.1 Overladelse til databehandlere

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”, persondatalovens § 41, stk. 4, 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. ”*

Typisk tolker man krigsregelen således, at hvis databehandlingen indeholder følsomme oplysninger og vedrører en større del af befolkningen, er den omfattet af krigsregelen.

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.

Er databehandlingen omfattet af krigsregelen, skal der etableres en løsning, som gør det muligt at slette data hos databehandleren, hvis det bliver nødvendigt.

## 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](https://fe-ddis.dk/cfcs/nyheder/arkiv/2015/Pages/NysikkerhedsanbefalingIt-sikkerhedp%C3%A5rejsen.aspx)”, 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 ud over ens egen organisation.

Det er derfor vigtigt, at man ved, hvor grænserne for ens egen organisation går og hvilke muligheder, der er for at kommunikere sikkert med andre parter.

## 10.1 Intern kommunikation

Inden for den enkelte organisation, f.eks. en region eller en kommune beskytter man sit interne netværk mod trusler fra internettet med firewalls og andre tekniske sikringsforanstaltninger.

Det er muligt at sende fortrolige eller følsomme oplysninger til andre medarbejdere med elektronisk post, f.eks. fra et sygehus til et andet, hvis kommunikationen kun sker via det interne netværk, men det er vigtigt, at man informerer medarbejderne om, hvilke forudsætninger, der gælder for den interne kommunikation.

Hvis man som medarbejder er i tvivl om, hvorvidt de oplysninger, man vil sende, kommer til at forlade det interne netværk, kan man henvende sig til organisationens it-afdeling.

## 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 Det åbne internet

Når offentlige myndigheder kommunikerer via det åbne internet 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 enten være en hemmelig softwarenøgle eller noget fysisk så som en token eller et papirnøglekort, som det, der anvendes i NemID.

Det kan sikres ved at anvende [sikker e-mail](https://www.nemid.nu/dk-da/om_nemid/hvad_er_nemid/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 kommunikation over det åbne net, men det anbefales, at private, f.eks. privatpraktiserende læger, anvender samme løsning, når de kommunikerer følsomme eller fortrolige oplysninger via internettet.

Hvis en offentlig myndighed kommunikerer med en borger via det åbne internet, skal det som udgangspunkt ske krypteret til dennes e-boks. Hvis dette ikke er muligt, skal borgeren oplyse en sikker e-mailadresse, der kan sendes krypteret til. 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 (SSL) tunneller, som etableres bilateralt mellem 2 organisationer.

Hvis man er i tvivl om, hvilke løsninger, ens organisation har etableret til at sende sikker post, 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 sundhedspesoner på portalen.

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

*VAN (Value Added Network) er en ældre teknologi, der i stort omfang bruges til at udveksle MedCom-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[[3]](#footnote-3) og et MPLS-net. For at blive tilsluttet sundhedsdatanettet skal der etableres en forbindelse til nettet fra ens eget, sikrede netværk, fx regionsnet.

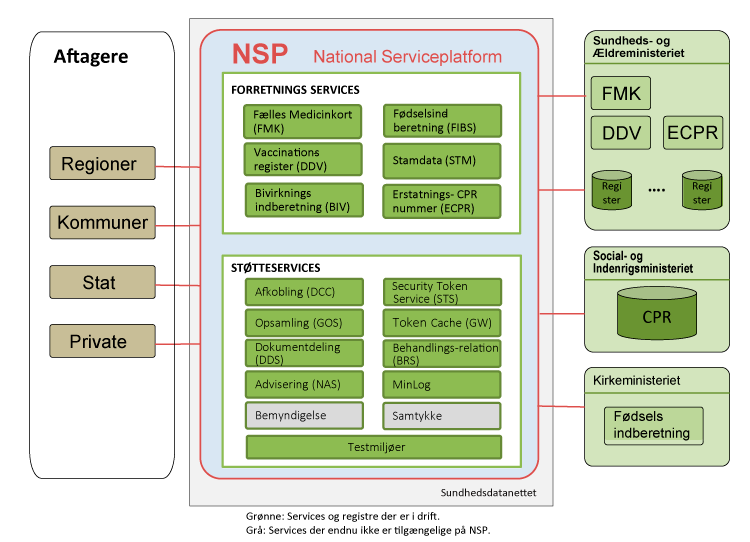
Da der som oftest er tale om følsomme personoplysninger, der kommunikeres, anbefales det, at de dataansvarlige/serviceudbyderne anvender endepunktskryptering (SSL/TLS) mellem server og klient, så udefra kommende ikke kan få adgang til oplysningerne.

### 10.3 Den nationale serviceplatform

Via sundhedsdatanettet kan man bl.a. få adgang til Den Nationale Serviceplatform (NSP)[[4]](#footnote-4).

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.

*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.*

****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. virus og malware, fordi man tilgår internettet fra åbne eller halvåbne internetforbindelser i toget, på et hotel eller til et møde ude i byen.

Mange anvender i dag smartphones, tablets eller bærbare PC-ere 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, giver det mulighed 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.

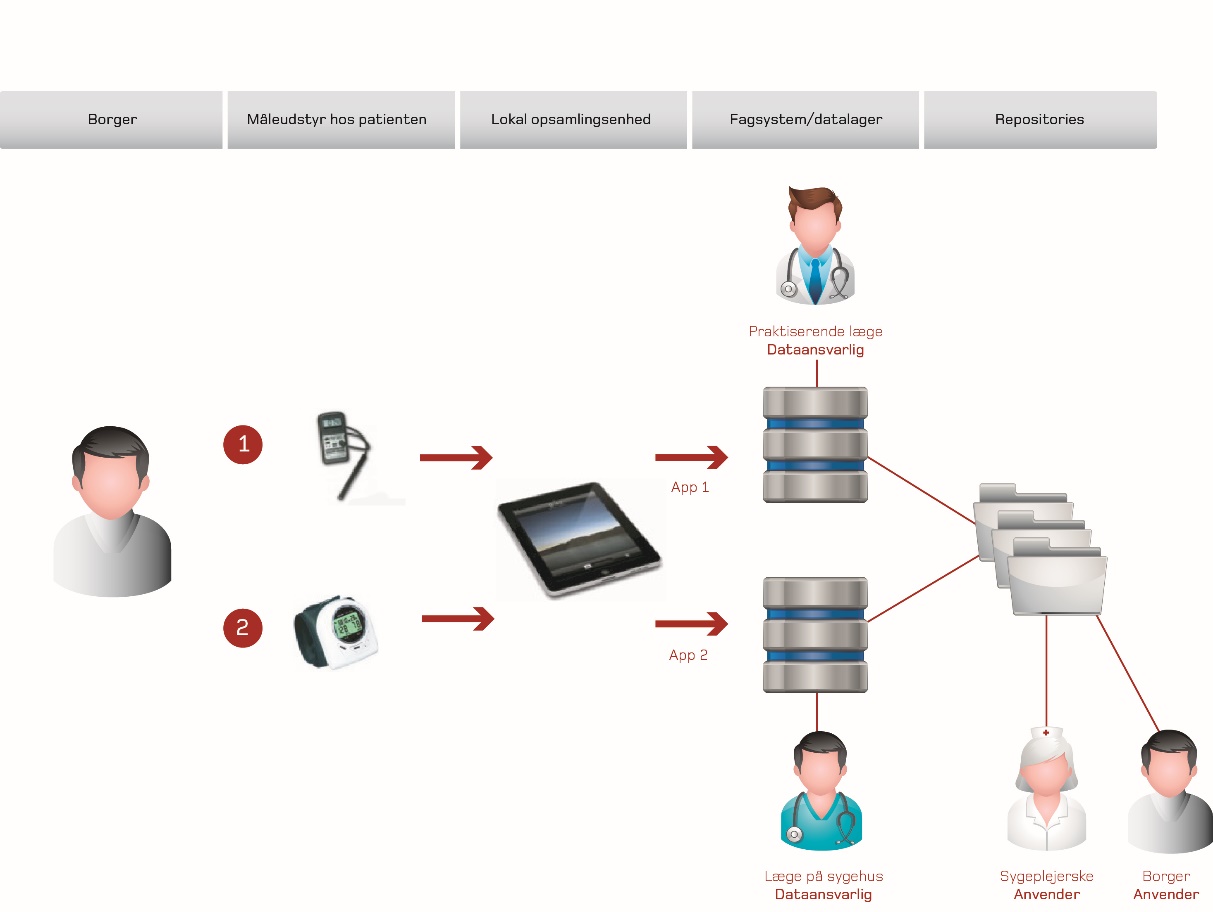
Virus og malware kan ligesom på en PC komme ind på den mobile enhed enten gennem et link eller en vedhæftet fil i ens mailprogram, eller når man downloader og installerer programmer (apps).

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 overholder [sikkerhedsbekendtgørelsens](https://www.retsinformation.dk/forms/r0710.aspx?id=842) 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 udstyr eller 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 virusopdatering 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.

*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. Regionerne har tilkendegivet, at de også vil anvende standarden som ramme for arbejdet med informationssikkerhed.

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 kommuner eller 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.

Anvendelse af standarden skal tilpasses den enkelte organisation. Der kan være forskel på, hvad der er nødvendigt for at have et tilstrækkeligt sikkerhedsniveau, alt efter størrelse og type af organisation.

Standarden indeholder en række kontrolmål, der dækker følgende områder:

* Politik
* Organisering af informationssikkerhed
* Personalesikkerhed
* Styring af aktiver
* Kryptografi
* Fysisk sikring og miljøsikring
* Driftssikkerhed
* Kommunikationssikkerhed
* Anskaffelse, udvikling og vedligeholdelse af systemer
* Leverandørforhold
* Styring af informationssikkerhedsbrud
* Beredskab og retablering
* Overensstemmelse med lov- og kontraktkrav

Digitaliseringsstyrelsen har udgivet flere [vejledninger](http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Vejledninger-om-sikkerhedsarbejdet/Informationssikkerhedspolitik), som kan understøtte organisationens implementering af ISO27001-standarden, f.eks.

### 12.2.1. Ledelsesværktøj

ISO27001 lægger vægt på, at det er organisationens ledelse, der tager ansvaret for informationssikkerhed i organisationen. 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 og det er herudfra, at man vurderer, om der er behov for at etablere (yderligere) sikringsforanstaltninger og hvilke.

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 virus, 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](https://fe-ddis.dk/CFCS/Pages/cfcs.aspx) 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 awareness kampagner og undervise medarbejderne i, hvordan de kan sikre sig mod at blive ofre for et hacker- eller virusangreb.

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.

#### 12.3.1.2 Anvendelse af cloud-baseret løsninger

Hvis der anvendes produkter som Projectplace, Dropbox o.l. i forbindelse med et projekt, skal man være opmærksom på, at disse løsninger ikke opfylder 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 Datatilsynets [krav](http://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/behandling-af-personoplysninger-i-cloud-loesningen-office-365/), herunder at der er indgået en databehandleraftale eller en EU-standardkontrakt, hvis der er tale om en leverandør i et usikkert tredjeland.

## 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

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 følsomme 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.

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](https://sundhedsstyrelsen.dk/da/medicin/medicinsk-udstyr/lovgivning-og-vejledning/sundhedsstyrelsens-vejledninger/vejledning-til-fabrikanter-af-medicinsk-udstyr-i-klasse-i#Hvorfor skal medicinsk udstyr CE-mærkes). 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](https://sundhedsstyrelsen.dk/da/medicin/medicinsk-udstyr/lovgivning-og-vejledning/sundhedsstyrelsens-vejledninger/~/media/53F2E52FB94C4BE495213EF0ED013A59.ashx), 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 rigtigt 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.

Mange eksisterende it-løsninger i sundhedsvæsenet har ikke de tilstrækkelige 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

Love, lovbekendtgørelser, bekendtgørelser og vejledninger tilgængelige på [www.retsinformation.dk](http://www.retsinformation.dk) .

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,* lovbekendtgørelse 1040 af 3. september 2014. Lokaliseret d. 4. januar 2016 på <https://www.retsinformation.dk/Forms/r0710.aspx?id=164756>. S. 8.

*Arkivloven,* lovbekendtgørelse nr. 1035 af 21. august 2007. Lokaliseret d. 4. januar 2016 på <https://www.retsinformation.dk/forms/r0710.aspx?id=12066>. S. 38.

[*Autorisationsloven*](https://www.retsinformation.dk/forms/r0710.aspx?id=138178), lovbekendtgørelse nr. 877 4. august 2011. Lokaliseret d. 4. januar på <https://www.retsinformation.dk/Forms/R0710.Aspx?id=138178>. S. 8

*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>. S. 10.

*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>. S. 19.

*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>. S. 14, 15.

*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>. S. 16, 22.

*Forældreansvarsloven,* Lovbekendtgørelse nr. 1820 af 23. december 2015. Lokaliseret d. 4. januar 2016 på

<https://www.retsinformation.dk/forms/R0710.aspx?id=173278>. S. 34.

*Journalføringsbekendtgørelsen,* bekendtgørelse nr. 3 af 2. januar 2013. Lokaliseret d. 4. januar på <https://www.retsinformation.dk/Forms/R0710.aspx?id=144978>. S. 10.

*Lægemiddelloven,* lovbekendtgørelse nr. 506 af 20. april 2013. Lokaliseret d. 4. januar 2016 på <https://www.retsinformation.dk/Forms/r0710.aspx?id=146586>. S. 8.

*Persondataloven*, lov nr. 429 af 31. maj 2000. Lokaliseret d. 4 januar 2016 på <https://www.retsinformation.dk/Forms/R0710.Aspx?id=828>. S. 8, 39.

*Retsplejeloven,* Lovbekendtgørelse nr. 1255 af 16. november 2015. Lokaliseret d. 4. januar 2016 på <https://www.retsinformation.dk/Forms/R0710.Aspx?id=172923>. S. 35.

*Retssikkerhedsloven (Lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter).* Lokaliseret 18. januar 2016 på <https://www.retsinformation.dk/Forms/R0710.aspx?id=1834>

*Serviceloven*, lovbekendtgørelse 1284 af 17. november 2015. Lokaliseret 18. januar 2016 på https://www.retsinformation.dk/Forms/R0710.aspx?id=175036. S. 8.

*Sikkerhedsbekendtgørelsen,* bekendtgørelse nr. 528 af 15. juni 2000. Lokaliseret d. 4. januar 2016 på <https://www.retsinformation.dk/forms/R0710.aspx?id=842>. S. 17, 37, 48.

*Sundhedsloven*, lovbekendtgørelse nr. 1202 af 24. november 2014. Lokaliseret d. 4. januar 2016 på <https://www.retsinformation.dk/Forms/r0710.aspx?id=152710>. S. 8.

*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 (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>. S. 44.

Danske Regioner (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>

Datatilsynet (2008/2015). *Binding Corporate Rules (BCR).* Lokaliseret d. 4. januar 2016 på <http://www.datatilsynet.dk/erhverv/tredjelande/binding-corporate-rules-bcr/>. S. 43.

Datatilsynet (2008/2015). *Blanket til øvrige offentlige anmeldelser.* Lokaliseret d. 4. januar 2016 på

<http://www.datatilsynet.dk/blanketter/offentlig-sektor/blanket-til-oevrig-offentlig-virksomhed/blanket-til-oevrige-offentlige-anmeldelser/>. S. 26.

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 (2008/2015). *Datatilsynets krav og anbefalinger i forbindelse med overførsel af personoplysninger via internettet i den private sektor.* Lokaliseret 4. januar 2016 på <http://www.datatilsynet.dk/erhverv/internettet/krav-og-anbefalinger-ifm-overfoersel-af-personoplysninger-via-internettet/>. S. 17.

Datatilsynet (2008/2015). *Kommissionens standardkontrakter.* Lokaliseret d. 4. januar 2016 på <http://www.datatilsynet.dk/erhverv/tredjelande/kommissionens-standardkontrakter/>. S. 43.

Datatilsynet (2015). *Kritik af Region Midtjyllands indberetning af fælles elektronisk patientjournal.* Lokaliseret d. 4. januar på <http://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/vedroerende-region-midtjyllands-faelles-elektroniske-patientjournal-midtepj/>. S. 11.

Datatilsynet (2013/2015). *Sikre tredjelande.* Lokaliseret d. 4. januar 2016 på <http://www.datatilsynet.dk/erhverv/tredjelande/sikre-tredjelande/>. S. 43.

Digitaliseringsstyrelsen (2015). *Informationssikkerhedspolitik.* Lokaliseret 18. januar 2016 på <http://www.digst.dk/Arkitektur-og-standarder/Videnscenter-for-implementering-af-ISO27001/Vejledninger-om-sikkerhedsarbejdet/Beredskabsplanlaegning.aspx>. S. 51.

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/> .S. 45.

***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>. S. 8.

Indenrigs- og Sundhedsministeriet (2007). *Oversigt over de juridiske rammer for adgangen til EPJ og IT-anvendelsen i sundhedsvæsenet*. Lokaliseret d. 4. januar 2016 på <http://www.medcom.dk/dwn1460>. S. 11.

Lægemiddelstyrelsen (2009/2015). *Vejledning til fabrikanter af medicinsk udstyr i klasse I.* Lokaliseret d. 4. januar 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](http://laegemiddelstyrelsen.dk/da/udstyr/lovgivning-og-vejledning/sundhedsstyrelsens-vejledninger/vejledning-til-fabrikanter-af-medicinsk-udstyr-i-klasse-i%23Hvorfor%20skal%20medicinsk%20udstyr%20CE-mærkes). S. 53.

Lægemiddelstyrelsen/Sundhedsstyrelsen (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>. S. 53.

MedCom (2015). *Infrastruktur.* Det danske sundhedsdatanet.Lokaliseret d. 4. januar 2016 på <http://medcom.dk/wm110009>. S. 46.

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>. S. 37.

Statens Serum Institut (2014). *Vejledning i adgang til registerdata hos Statens Serum Instituts Forskerservice,* udkast*.* Lokaliseret d. 4. januar 2016 på <http://www.ssi.dk/~/media/Indhold/DK%20-%20dansk/Sundhedsdata%20og%20it/NSF/Forskerservice/Vejledning%20Forskerservice.ashx>. S. 38.

Sundhedsdatastyrelsen (2016). *National Sundheds-It drfitstatus.* Lokaliseret 4. januar 2016 på <https://www.nspop.dk/display/driftsstatus/Driftsstatus>. S. 46.

Sundhedsstyrelsen (2011). *Smitsomme sygdomme med cpr-baseret anmeldepligt.* Lokaliseret d. 4. januar 2016 på <https://sundhedsstyrelsen.dk/da/sundhed/smitsomme-sygdomme/~/media/056EABDB272945A38BBF13470C43A61F.ashx>. S. 11.

Videnskabsetisk Komitésystem: [Anmeldelsesportal](http://www.drvk.dk/anmeldelse/Anmeldelse.html), s. 37 – Lokaliseret 18. januar 2016 på http://www.drvk.dk/anmeldelse/Anmeldelse.html

1. Indenrigs- og Sundhedsministeriet: Oversigt over de juridiske rammer for adgangen til EPJ og IT-anvendelsen i sundhedsvæsenet

   <http://www.medcom.dk/dwn1460> [↑](#footnote-ref-1)
2. Sundhedspersoner, der *ikke* er læger, tandlæger, jordemødre, sygeplejersker, sundhedsplejersker, social- og sundhedsassistenter, radiografer eller ambulancebehandlere med særlig kompetence [↑](#footnote-ref-2)
3. Læs mere på http://medcom.dk/wm110009 [↑](#footnote-ref-3)
4. Læs mere på nspop.dk [↑](#footnote-ref-4)