SUNDHEDSDATA-
STYRELSEN

Vejledning om informationssikkerhed

Birgitte Drewes, afdelingschef, Sundhedsdatastyrelsen
Marchen Lyngby, fuldmægtig, Sundhedsdatastyrelsen

Vejledningen kan downloades her: http://sundhedsdatastyrelsen.dk/da/rammer-og-retningslinjer/om-informationssikkerhed

Baggrund

6) videregivelsen sker til en læge, tandlæge eller jordemoder om en patient, som modtageren tidligere har deltaget i behandlingen af, når
a) videregivelsen er nødvendig og relevant til brug for evaluering af modtagerens egen indsats i behandlingen eller som dokumentation for erhvervede kvalifikationer i et uddannelsesforløb

SUNDHEDSDATA-STYRELSEN

- Sundhedsstyrelsens vejledning 2008
- Ændringer i sundhedsloven
- Øget digitalisering i sundhedsvæsenet

Fremgangsmåde

SUNDHEDSDATA-STYRELSEN

Arbejdsgruppe med repræsentanter fra Sundheds- og Ældreministeriet, kommuner, regioner, praktiserende læger, industrien, MedCom og sundhed.dk

Opstartsseminar maj 2015

7 arbejdsmøder

- **Oplæg/drøftelse**
- **Udkast**
- **Godkendelse**

Intern høring december 2015

Offentlig høring februar 2016

515 kommentarer fra ca. 40 organisationer indarbejdet

Ændringer

SUNDHEDSDATA-
STYRELSEN

- Fra DS 484 til ISO 27001
- Fokus på hele sundhedsvæsenet
- Fokus på lovgrundlag
- Fokus på at henvise til autoritative kilder

Målgruppe

- Ansvarlige for data- og informationssikkerhed (regioner, kommuner, praksis, apoteker mv.)
- It-funktioner
- Leverandører

- Ikke primært rettet til medarbejdere
  - Udarbejdelse af behovsbaseret informationsmateriale baseret på fælles forståelse i vejledning
  - Meget gerne dialog med SDS

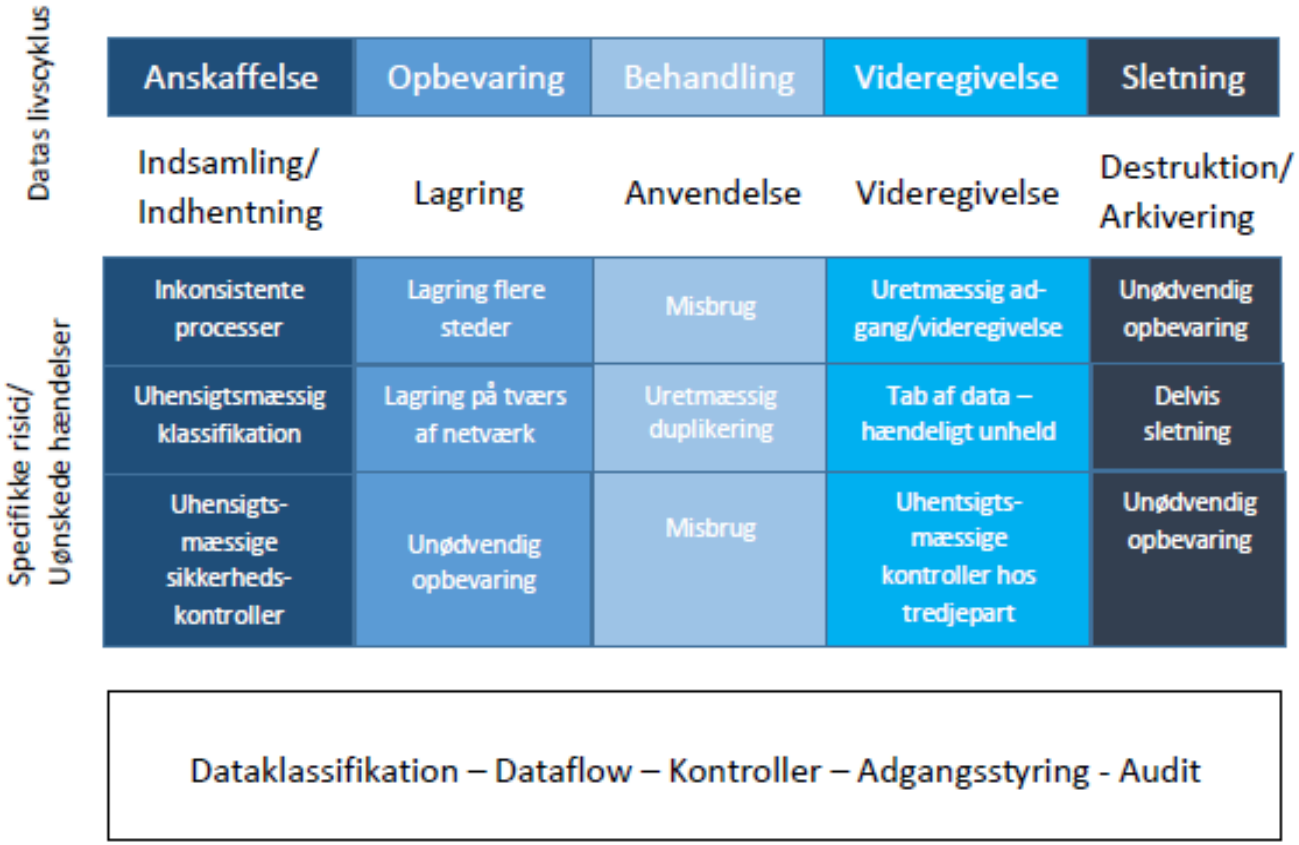
Indhold i vejledningen

- Adgang til oplysninger – lovkrav
- Dataansvar
- Deling af oplysninger på tværs af sektorer
- Adgang til borgerens oplysninger
- Borgerens adgang til oplysninger
- Anvendelse af patientoplysninger til videnskabeligt eller statistisk formål
- Overførsel af patientoplysninger til EU- og tredjelande
- Netværkssikkerhed
- Mobil sikkerhed
- Krav vedr. informationssikkerhed

Dataansvar

SUNDHEDSDATA-STYRELSEN

- Forpligtelser
- Hjemmel
- Databehandlere
- Anmeldelse til Datatilsynet
- Dataflow/databeskrivelse



Lovgrundlag

- Beskrivelse og tolkning af lovgrundlaget
- Anbefalinger til, hvordan man etablerer et tilstrækkeligt sikkerhedsniveau
- Anbefalinger til videre læsning
- Afvejning mellem informationssikkerhed og andre forretningsmål

SUNDHEDSDATA-STYRELSEN

Sundhedsloven	•I sundhedsloven fastlægges reglerne for indhentning/videregivelse og behandling af patientoplysninger •Sundhedsloven er den primære lov på sundhedsområdet
Persondataloven	•Persondataloven beskriver de generelle regler for behandling af personoplysninger •Persondataloven bygger på EUs persondatadirektiv •Persondataloven finder anvendelse, hvor der ikke er anden lovgivning, der regulerer behandlingen, herunder indhentning af personoplysninger
Autorisationsloven	•Autorisationsloven beskriver rammerne for sundhedspersoners pligter, herunder journalføring
Retssikkerhedsloven	•Retssikkerhedsloven indeholder regler om samtykke på det sociale område •Retssikkerhedsloven indeholder bestemmelser om udveksling af oplysninger om indlæggelse/udskrivning fra sygehuse
Serviceloven	•I serviceloven findes regler for udveksling af oplysninger i det forebyggende arbejde med børn og unge
Lægemiddelloven og Apotekerloven	•Lægemiddelloven og Apotekerloven indeholder regler for indsamling og behandling af lægemiddeloplysninger
Forvaltningsloven	•Indeholder generelle bestemmelser om offentligt ansattes tavshedspligt

Adgang til oplysninger - lovkrav

SUNDHEDSDATA-STYRELSEN

- Behandlingsøjemed
  - Videregivelse
  - Elektronisk indhentning
- Sekundær anvendelse
  - Administration
  - Videnskabelige og statistiske undersøgelser
- Videregivelse til tilsynsmyndigheder og til behandling af klage- og erstatningssager
- Videregivelse til politiet
- Andet

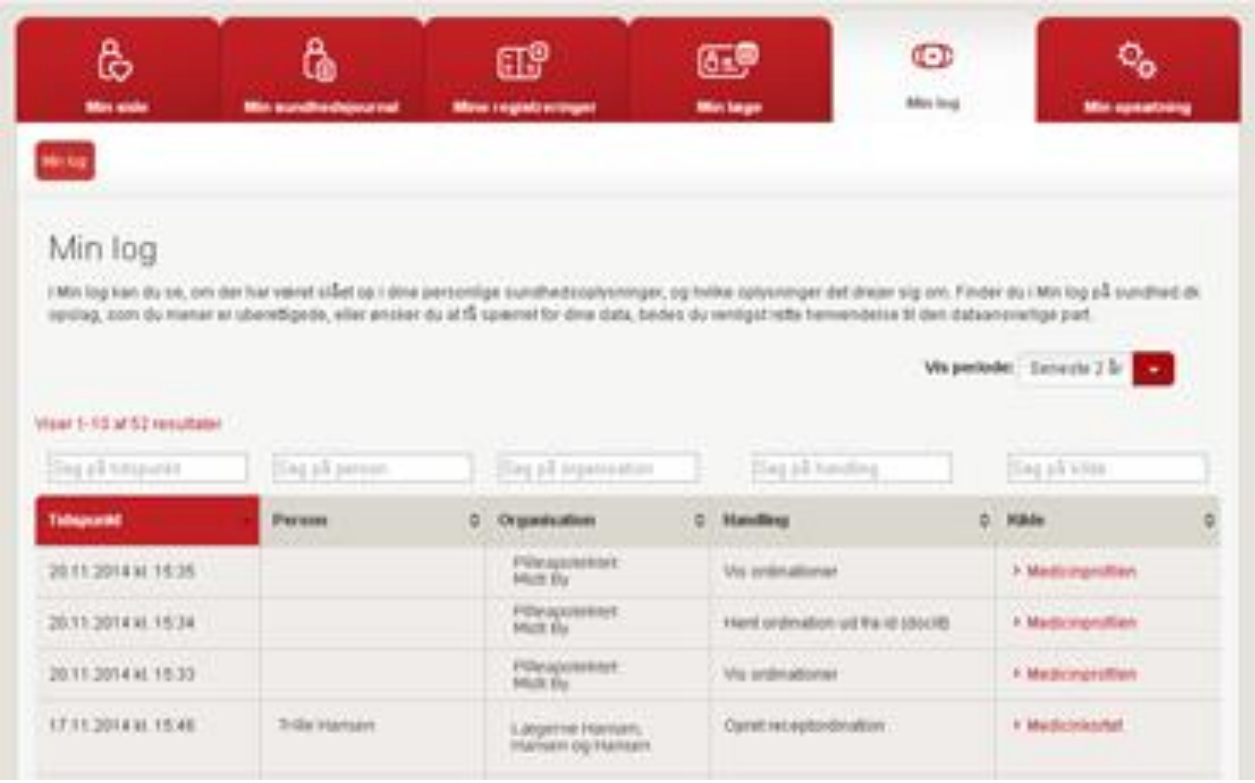
Deling af oplysninger på tværs

SUNDHEDSDATA-STYRELSEN

- Deling = videregivelse eller indhentning
- Data deles via:
  - Mail
  - MedCom meddelelser
  - Landsdækkende databaser
  - andet
- Aftaler mellem parterne
- Afklaring af ansvarsområder

Borgerens adgang til egne oplysninger

SUNDHEDSDATA-STYRELSEN



- Indsigtsret
- Adgang til egne sundhedsoplysninger
- Adgang til logoplysninger
- Adgang for pårørende/værger
- Samtykke og fuldmagt

Videnskabelige og statistiske formål

SUNDHEDSDATA-STYRELSEN

- Sundhedsvidenskabelig forskning på mennesker og biologisk materiale
- Videnskabelige undersøgelser på basis af patientjournaler
- Registerforskning
- Biobanker
- Opbevaring – sikkerhed
- Videregivelse
- Pseudonymisering/anonymisering
- Big Data

Næste skridt

SUNDHEDSDATA-
STYRELSEN

- Kommunikationsplan
  - Er lagt på Sundhedsdatastyrelsens hjemmeside
  - FAQ
  - Seminarer efterår 2016
  - Dialogmøder
- Redaktionsgruppe
  - Mødes i efteråret 2016 og lægger plan
    - EU-forordningen
    - Kvalitetsarbejde?

Hvad er forordningen?

SUNDHEDSDATA-STYRELSEN

- Persondataloven bygger på et europæisk direktiv fra 1995
- Direktivet erstattes af en ny databeskyttelsesforordning, som skal gælde horisontalt i både den private og offentlige sektor (databeskyttelsesforordningen)
- En forordning gælder ”som den er”, dvs. den skal ikke oversættes til en dansk lov
- Forordningen lå færdig i december 2015 og trådte i kraft 25. maj 2016
- Pakken får virkning 2 år efter ikrafttrædelsen, dvs. 25. maj 2018.

Hvad er nyt?

SUNDHEDSDATA-
STYRELSEN

- Med forordningen sker der i vidt omfang en videreførelse og præcisering af, hvad der allerede gælder i Danmark i dag. Det er f.eks. tilfældet med reglerne om, under hvilke betingelser der må behandles personoplysninger, og hvordan personoplysninger skal beskyttes.

- Der indføres en række mindre nye krav.

Kapitel 1 – hvilke data?

SUNDHEDSDATA-STYRELSEN

- Persondata, som i dag

- Behandling af personoplysninger på internettet om EU-borgere vil i højere grad end i dag være omfattet af forordningens regler.
  - også, selv om den dataansvarlige eller en databehandler ikke er etableret inden for EU's grænser.

Kapitel 2 – Grundlæggende principper for behandling af data

SUNDHEDSDATA-STYRELSEN

- Helt overordnet svarer forordningens behandlingsregler i vidt omfang til reglerne i det gældende direktiv.

- Der vil stadig blive sondret mellem almindelige personoplysninger og følsomme personoplysninger

- Man vil stadig kunne behandle relevante personoplysninger til saglige formål bl.a. på baggrund af et udtrykkeligt samtykke fra den person, oplysningerne vedrører, eller når det er nødvendigt at behandle oplysningerne med henblik på myndighedsudøvelse.

Kapitel 3 – Den registreredes rettigheder

SUNDHEDSDATA-STYRELSEN

- Der vil stadig være en pligt for den dataansvarlige til at oplyse den registrerede om, at der behandles oplysninger om den pågældende, samt en ret for den registrerede til at få indsigt i oplysninger om sig selv, til at få slettet eller berigtiget urigtige oplysninger og til at gøre indsigelse mod, at oplysninger behandles.

Kapitel 4 – Den dataansvarliges forpligtelser

SUNDHEDSDATA-STYRELSEN

- Reglerne bygger -som noget nyt -udtrykkeligt på en risikobaseret tilgang. Graden af risikoen for den registreredes grundlæggende rettigheder, herunder retten til privatliv, er bestemmende for, hvilke sikkerhedsforanstaltninger en given behandling kræver.
- Der skal være passende sikkerhedsforanstaltninger bl.a. mod, at uvedkommende får adgang til personoplysninger.
- Der vil i visse tilfælde være krav om, at der forud for en behandling af personoplysninger skal udarbejdes en konsekvensanalyse, som skal kortlægge risiciene for de registrerede. Viser en konsekvensanalyse, at der vil være en høj risiko for den registrerede, skal tilsynsmyndigheden høres, inden behandlingen iværksættes.
- Den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger designet til at understøtte databeskyttelse (”data protection by design and by default”).
- Dataansvarlige offentlige myndigheder skal udpege en såkaldt databeskyttelsesrådgiver, som bl.a. skal rådgive den dataansvarlige og databehandleren om behandlingen af personoplysninger.
- Dataansvarlige skal anmelde brud på datasikkerheden til tilsynsmyndigheden, ligesom de registrerede i visse tilfælde skal underrettes herom.

Kapitel 5 – Overførsel til tredjelande

- Reglerne bygger i vid udstrækning på reglerne i det gældende direktiv.

Kapitel 6 og 7 - Tilsyn

SUNDHEDSDATA-STYRELSEN

- Reglerne bygger i vid udstrækning på reglerne i det gældende direktiv.

- Forordningen indeholder en væsentlig udbygning af tilsynsmyndighedernes europæiske samarbejde.

- Der oprettes bl.a. et Europæisk Databeskyttelsesråd, som sammensættes af repræsentanter fra medlemsstaternes tilsynsmyndigheder, og som i visse sager kan træffe afgørelser, som er bindende for de nationale tilsynsmyndigheder.

Kapitel 8 - Straf

SUNDHEDSDATA-STYRELSEN

- Som noget nyt indeholder forordningen bestemmelser om, at tilsynsmyndighederne kan udstede administrative bøder på op til 20.000.000 euro eller 4 pct. af årlig global omsætning, hvis forordningens bestemmelser overtrædes.

- En ordning med *administrative* bøder giver anledning til grundlovsmæssige betænkeligheder for Danmark. Der er på den baggrund i forordningen tilføjet en bestemmelse, som giver mulighed for at implementere bestemmelserne om administrative bøder i det nationale *strafferetlige* system.

Kapitel 9 – Forskning og Statistik mv.

SUNDHEDSDATA-STYRELSEN

- Det er Justitsministeriets foreløbige vurdering, at det efter bestemmelserne i kapitel 9 sammenholdt med forordningens generelle bestemmelser i vidt omfang vil være muligt at behandle personoplysninger til videnskabelig forskning, herunder registerbaseret forskning, samt til statistik på samme måde som i dag.

Hvis du ikke husker andet

SUNDHEDSDATA-
STYRELSEN

- Hvis I har godt styr på persondatalov og ISO 27001 i dag vil I have godt styr på forordningen
- Hvis det ikke er dokumenteret, findes det ikke

SUNDHEDSDATA-
STYRELSEN

Spørgsmål??

Informationssikkerhed@sundhedsdata.dk

Vejledningen kan downloades her: http://sundhedsdatastyrelsen.dk/da/rammer-og-retningslinjer/om-informationssikkerhed