Manual til implementering af EU Persondataforordningen

1 Formål

Formålet med denne manual er at hjælpe klinikker, der selv ønsker at stå for arbejdet med at implementere EU persondataforordningen.

Anbefalingerne tager udgangspunkt i Justitsministeriets betænkning (analyse og tolkning af hvordan EU persondataforordningen kan integreres i den danske lovgivning), den nye fremsatte databeskyttelseslov, der forventes vedtaget i starten af 2018 samt vejledninger udarbejdet af Datatilsynet.

Hvis du som klinikejer er i tvivl om retsgrundlaget, bør du opsøge juridisk bistand.

2 Generelle betragtninger

EU Persondataforordningen er lavet for at beskytte os som borgere i en digital verden mod, at vores personoplysninger opbevares usikkert og deles med andre uden vores viden eller tilladelse.

Som klinik er du dataansvarlig, når du behandler personoplysninger om både ansatte og patienter. Personoplysninger opdeles i "almindelige" og "følsomme" oplysninger, og i Danmark har vi en særlig kategori, hvor CPR. nr. hører under.

Efter forordningen, skal man foretage "passende organisatoriske og tekniske sikkerhedsmæssige foranstaltninger", når man behandler personoplysninger digitalt. Som klinikejer skal du antage en risikobaseret tilgang, når du skal tage stilling til, hvilke foranstaltninger du skal foretage for at sikre patientens og den ansattes data.

Det vil sige, at du, hver gang du behandler (indhenter, opbevarer eller videregiver) personoplysninger, skal overveje, om du har bemyndigelse til at gøre det, og alt efter typen af data skal du overveje risikoen for, at oplysningerne lækkes og konsekvenserne af et evt. læk i forhold til personen.

Hvis man har meget data, der er *personfølsomt* (herunder helbredsoplysninger, fagforeningsforhold, race og etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, biometrisk data med henblik på identifikation og seksuelle forhold) forventer myndighederne, at du er særlig omhyggelig i forhold til sikring af data.

Det er her, du skal foretage en risikobaseret vurdering i forhold til at få fastlagt "rimelige" sikkerhedsmæssige foranstaltninger. Fx giver det mening, at en lokal jagtklub passer bedre på/sikrer sin medlemsliste end den lokale fodboldforening, da det må formodes, at der formenligt findes skydevåben på jagtklubbens medlemmers adresser.

3 Liste over punkter man skal igennem

a. Data-flow analyse
b. Risikovurdering (konsekvensanalyse)

c. Fortegnelse over behandlingsaktiviteter
d. Informationssikkerhedspolitik / IT-sikkerhedspolitik
e. Implementering

ad a) Data-flow analyse

En data-flow analyse kan laves mere eller mindre omfattende. Formålet med data-flow analysen er at skabe et overblik over dine behandlinger af personoplysninger i klinikken. Har du hyret et eksternt firma til at hjælpe med denne del, vil de bl.a. kortlægge data-flow med en række spørgsmål til de forskellige mennesker i klinikken, der fx har med patientbehandling, personaleadministration og regnskab at gøre. Det kan kobles med en GAP-analyse, hvor man kortlægger mangler i forhold til overholdelse af forordningen.

Det er ikke et specifikt krav i persondataforordningen, at der laves en data-flow analyse, men det er en stor hjælp i forhold til at kortlægge, hvilke arbejdsgange man har, hvor der behandles (indhentes, opbevares eller videregives) personoplysninger. En data-flow analyse gør det også nemmere at lave den interne "fortegnelse" over behandlingsaktiviteter, som ER et krav jf. forordningen.

Der er vedhæftet hjælpeværktøj til data-flowanalysen (excel ark).

ad b) Risikovurdering (konsekvensanalyse)

Der er ikke krav om, at du som klinikejer laver en risikovurdering. Men af hensyn til fastlæggelse af en IT-politik anbefales det, at du laver en risikovurdering af de primære aktiviteter, hvor du behandler personoplysninger særligt, hvis man behandler personoplysninger af følsom karakter.

Formålet med risikovurderingen er at vise, at du som klinikejer har et overblik over de sikkerhedstiltag, du har foretaget for at gøre beskyttelsen af personoplysningerne tilstrækkelig. Du kan efterfølgende tage udgangspunkt i risikovurderingen, når du fastlægger din IT politik.

Det er heller ikke nødvendigt for mindre klinikker at have en databeskyttelsesrådgiver (DPO/Data Protection Officer). Man kan dog sagtens vælge at udpege en DPO på frivillig basis. Datatilsynet har ikke sat en omsætningsgrænse eller et antal fuldtidsansatte læger/kiropraktorer i forhold til, hvornår man er en mindre klinik, og hvornår man ikke er, så det beror på et skøn.

Vedhæftede excel-ark har inkorporeret et risikovurderingsværktøj.

ad c) Fortegnelse over behandlingsaktiviteter

Det er et krav, at alle dataansvarlige og databehandlere fører interne fortegnelser over al behandling af personoplysninger, dvs. både almindelige personoplysninger og følsomme personoplysninger. Fortegnelsen skal kun sendes til Datatilsynet, hvis du bliver bedt om det. Du skal have både en elektronisk og en fysisk udgave af fortegnelsen.

Fortegnelsen skal som minimum indeholde:

- Kontaktoplysninger for den dataansvarlige – og hvis relevant, fælles dataansvarlige, den dataansvarliges repræsentant og databeskyttelsesrådgiver.
- Formål med behandlingen af oplysningerne (f.eks. personaleadministration, journalføring).
- Kategorier af registrerede (f.eks. oplysninger om nuværende og tidligere medarbejdere eller patienter) og kategorier af personoplysninger (f.eks. identifikationsoplysninger, oplysninger om løn, arbejdstid, cpr.nr. m.v.).
- Kategorier af modtagere ved videregivelse (f.eks. SKAT, FHC m.v.).
- Overførsler til tredjelande og internationale organisationer.
- Slettefrister/ forventede tidsfrister for sletning af de forskellige kategorier af oplysninger.
- Hvis muligt, en generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger (f.eks. individuelle brugernavne og passwords, procedurer og politikker for behandling og kommunikation af personoplysninger).

Du kan læse mere om fortegnelsen på dette link, blandt andet er der eksempel på en fortegnelse over behandlingsaktiviteter vedrørende HR:
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_om_fortegnelse__endelig___DOK461184_.PDF

ad d) Informationssikkerhedspolitik / IT-sikkerhedspolitik

Klinikkens informationssikkerhedspolitik skal tage udgangspunkt i lovgivningen og klinikkens risikovurdering.

Inspiration til indhold:

- ”Analyse af de tekniske og organisatoriske foranstaltninger”.
- Dansk Industri (DI) har lavet en implementerings guide der hedder ”Persondataforordningen formuleret som kontroller”. Se særligt side 25-28 om de registreredes rettigheder samt side 28-33 om virksomhedens forpligtelser og sørg for, at din IT-politik også bekriver, hvordan I vil imødekomme indsigtsforespørgsler, brud m.m. https://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Persondataforordningen%20formuleret%20som%20kontroller.pdf.
- ”Krav om datasikkerhed i forbindelse med personaleadministration” https://www.datatilsynet.dk/erhverv/personaleadministration/krav-om-datasikkerhed-i-forbindelse-med-personaleadministration/ .

ad e) Implementering

Når der sker brist i sikkerheden, kan det være, fordi en ansat ikke følger den fastlagte IT–sikkerhedspolitik, f.eks. sender personhenførbart data som navn eller cpr. nr. koblet med helbredsoplysninger via ikke krypteret mail.

Det er dig som klinikejer, der har ansvaret for at indskærpe reglerne, men også gøre det så nemt at overholde reglerne som muligt.

Eksempler, som kunne gøre det nemmere at overholde reglerne kunne være:

- At det teknisk blev sat op, så man ikke kan gemme talkombinationer, der ligner cpr. nr. på usikre drev.
- At man ikke skal have Dropbox installeret på klinikkens computere, så man ikke kommer til at gemme personfølsomme data (i skyen uden for EU) osv., eller
- At behovet for diskretion italesættes, at der skal passes på de personfølsomme data ligesom vi forventer, at ens egen læge passer på data om os.

4 Databehandleraftaler

Efter persondataforordningen er der krav om, at der skal indgås en skriftlig databehandleraftale mellem dataansvarlige og databehandler, hvori det er beskrevet hvem, der kan tilgå data, evt. erklæring om tavshedspligt, og hvordan data skal behandles/opbevares/slettes.

Du vil som klinikejer være dataansvarlig i forhold til en lang række personoplysninger, f.eks. om dine ansatte og dine patienter. Som dataansvarlig skal du blandt andet sikre dig:

- At du har lov til at behandle de oplysninger, som du og dine databehandlere er i besiddelse af.
- At du er i stand til at efterleve den registrerede persons rettigheder (f.eks. opfylde din oplysningspligt i forhold til, hvilke oplysninger du har om den pågældende)
- At du får indberettet eventuelle brud på persondatasikkerheden til Datatilsynet inden for 72 timer.

En databehandler er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne, dvs. at databehandleren f.eks. indsamler, registrerer, opbevarer, videregiver eller sletter personoplysninger efter instruks fra dig som klinikejer (dataansvarlig). Et eksempel på en databehandler kan være din systemleverandør til klinikkens journalsystem.

Databehandleraftalen skal sikre, at databehandleren kun behandler personoplysningerne på den måde, der er aftalt med og godkendt af dig, og det er dit ansvar at føre tilsyn med databehandleren.

Databehandleren har dog også et selvstændigt ansvar, derved at ”han” ikke må lave behandling af personoplysninger, der er ulovlige jf. forordningen, selvom det sker efter instruks fra den dataansvarlige.

Delt dataansvarlig
Man taler om delt dataansvar i de situationer, hvor du som klinik deler personoplysninger med en samarbejdspartner, f.eks. med Falck Healthcare eller i nogle situationer forsikringsselskaberne. I de situationer skal du være opmærksom på, at du ikke indtaster/videregiver personhenførbare

data koblet med fx helbredsoplysninger via usikre kanaler, og at du har lov til at videregive oplysningerne.

Skabelon til Datatilsynets nationale databehandleraftale vedlægges.

5 Samtykke

Samtykke efter persondataforordningen
Ud over reglerne i sundhedslovgivningen gælder også persondataforordningens regler om samtykke. Samtykke efter forordningen er udtryk for, at de registrerede gives et reelt valg og kontrol over, hvordan deres oplysninger bruges.

Samtykket skal være på plads, inden den dataansvarlige påbegynder behandling af de oplysninger, samtykket angår.

Med persondataforordningen er der krav om, at du skal oplyse den registrerede om nogle generelle rettigheder, f.eks. at et samtykke til hver en tid kan tilbagekaldes. Hvis den registrerede tilbagekalder sit samtykke til behandling af oplysninger, skal den dataansvarlige stoppe med at behandle oplysningerne.

Et samtykke skal være specifikt. Det betyder, at samtykket ikke må være generelt udformet eller uden præcis angivelse af formålene med behandlingen af personoplysningerne. Hvis en behandling af oplysninger tjener flere formål, skal den dataansvarlige indhente særskilt samtykke for hvert enkelt formål, som skal behandles på grund af den registreredes samtykke. Rent praktisk kan dette foregå ved en samlet erklæring, hvor den registrerede kan markere, hvilke formål den pågældende vil acceptere, der behandles oplysninger til. Tavshed, allerede afkrydsede felter på hjemmesider eller inaktivitet kan ikke ligestilles med et samtykke.

Som sundhedsfaglig behandler er det vigtigt at holde tungen lige i munden, når der skal skelnes mellem diverse former for samtykke, idet der ud over forordningens regler om samtykke også er regler om samtykke inden for sundhedsområdet, alt afhængigt af formålet med indhentelse af samtykket.

Samtykke til sundhedsfaglig behandling
Samtykke til undersøgelse og behandling (her menes sundhedsfaglig behandling som manuel behandling eller f.eks. en røntgenundersøgelse) kan gives mundtlig, skriftlig og kan i nogen sammenhænge også være stiltiende, men det skal altid journalføres. Samtykket skal altid være aktuel (givet til det konkrete formål) efter passende information, og derfor kan man ikke give skriftligt samtykke til sundhedsfaglig behandling på forhånd.

Gives der samtykke til en behandlingsplan, skal fornyet samtykke kun indhentes, hvis der afviges fra den oprindelige behandlingsplan. Altså behøver du ikke journalføre samtykke til hver eneste kontrol. Stiltiende samtykke bliver typisk accepteret, når man laver objektiv undersøgelse. I disse tilfælde skal du ikke bede om samtykke til alle delelementer som f.eks. strakt benløft-test, test af reflekser m.m.

Laves der undersøgelser som en del af udredningen, der er af mere invasiv karakter, f.eks. biopsi eller blodprøver, kræves der mere udtrykkeligt samtykke. Det gælder også ved f.eks. røntgenundersøgelse.

Du kan læse mere om samtykke på følgende link:
https://www.retsinformation.dk/Forms/R0710.aspx?id=21076

Samtykke til indhentning og videregivelse af helbredsoplysninger i forbindelse med behandling af patienten
Efter sundhedsloven kan man med patientens samtykke videregive helbredsoplysninger til andre sundhedspersoner i forbindelse med aktuel behandling. Samtykket kan være mundtlig eller skriftligt og kan afgives til den sundhedsperson, der videregiver oplysninger, eller til den sundhedsperson, der modtager oplysninger. Samtykket skal indføres i patientjournalen.

Den dataansvarlige skal kunne bevise, at der foreligger et udtrykkeligt samtykke, og det vil derfor være hensigtsmæssigt, at samtykket foreligger skriftligt. Ved at samtykket er skriftligt vil det nemt kunne dokumenteres over for f.eks. sygehusafdelinger, der måtte kræve det.

Du kan læse mere om samtykke ved indhentning og videregivelse af helbredsoplysninger på dette link:
https://www.retsinformation.dk/Forms/R0710.aspx?id=183932#idc101cee1-c9c0-4880-ac97-586a56134f56

Fra 2013 har kiropraktorer lovligt kunnet lave opslag i elektroniske systemer, de måtte have adgang til og i fornødent omfang indhente oplysninger om en patients helbredsforhold, øvrige rent private forhold og andre fortrolige oplysninger, når det er nødvendigt i forbindelse med aktuel behandling af patienten.

Se bekendtgørelse om kiropraktorers adgang til indhentning af helbredsoplysninger m.v. i elektroniske systemer. https://www.retsinformation.dk/Forms/R0710.aspx?id=145032

Samtykke til videregivelse af helbredsoplysninger til andre formål (end behandling)
Efter sundhedsloven og i bekendtgørelse om information og samtykke og om videregivelse af helbredsoplysninger mv. står der specifikt, at videregivelse til andre formål end sundhedsfaglig behandling (fx oplysninger om helbredsforhold til et forsikringsselskab) SKAL være skriftligt, og samtykket skal gives til den person, der er i besiddelse af og skal videregive oplysninger. Dvs. du skal sikre dig, at der foreligger relevant (skriftlig eller digital fx via NemId) samtykke til videregivelse, inden du videregiver helbredsoplysninger.

Se mere herom på: https://www.retsinformation.dk/Forms/R0710.aspx?id=21075

Formålet med manualen er at formidle informationer om persondataforordningen til klinikejerne.

DKF forsøger at sikre, at alle informationer er så præcise som muligt, men DKF fraskriver sig ethvert ansvar for tab eller skade, – såvel direkte som indirekte – der måtte opstå som følge af brugen af informationer fra manualen.