Persondataforordningsloven

Compliance rapport – Speciallægepraksis BA's interne retningslinjer

Speciallægepraksis BA er forpligtet til at beskytte fortroligheden, integriteten og tilgængeligheden af vores patienter og medarbejderes personoplysninger. Speciallægepraksis BA arbejder kontinuerligt med alle nødvendige tiltag for at sikre løbende overholdelse af persondataforordningen. Denne compliance rapport beskriver interne retningslinjer i Speciallægepraksis BA. Endvidere beskriver rapporten hvordan Speciallægepraksis BA opfylder kravene til persondataforordningen.

DEL 1: Persondataforordning

1.1 De 6 databeskyttelsesprincipper

I henhold til persondataforordningen 25. maj 2018 har Speciallægepraksis BA som dataansvarlig et juridisk ansvar for at:

1. Indsamle og behandle personoplysninger lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.
2. Personoplysninger indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål
3. Sikre, at personoplysninger er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de anvendes.
4. Opbevare personoplysninger nøjagtige, komplette og opdaterede; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de anvendes, straks slettes eller berigtiges
5. Opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger anvendes; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder (»opbevaringsbegrænsning«)
6. At sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger
7. Øvrig informationer vi holder os til: https://www.laeger.dk/sites/default/files/plo_informationssikkerhed_i_almen_praksis.pdf

1.2 Speciallægepraksis BA

Speciallægepraksis BA vil som dataansvarlig bestræbe sig på:

- At overholde både Persondataforordning og opfylde god databehandlingsskik
- At beskytte privatlivets rettigheder i overensstemmelse med Persondataforordningen for de personer, vi samarbejder med samt Speciallægepraksis BAs eget personale
- At sikre, at personoplysninger i Speciallægepraksis BA bevares sikkert og i aflåste rum
- At støtte personalet til at opfylde deres juridiske ansvar, som beskrevet i de 6 databeskyttelsesprincipper
- At respektere enkeltpersoners rettigheder

1.3 Databeskyttelsespolitik

Formålet med denne databeskyttelsespolitik er:

- At skitsere, hvordan Speciallægepraksis BA bestræber sig på at overholde Persondataforordning
- At give retningslinjer for god praksis for personalet
- At beskytte Speciallægepraksis BA fra konsekvenserne ved databrud

1.4 Databeskyttelsespolitik anvendelsesområde

Denne politik gælder for alle medarbejdere, der håndterer personoplysninger om de personer, vi samarbejder med og Speciallægepraksis BAs eget personale

DEL 2: Databrud

2.1 Introduktion

Et databrud kan ske af en række årsager, herunder:

- Tab eller tyveri af udstyr, som data er lagret på
- Upassende adgangskontrol tillader uautoriseret brug
- Udstyrssvigt
- Menneskelig fejl f.eks. misaddressing en e-mail eller indtastning af et forkert telefonnummer eller fax
- Uforudsete omstændigheder som f.eks. oversvømmelse eller brand
- Computer hacking
- Adgang, hvor information opnås ved bedrageri (fx hvor en person i samtalen trækker fortrolige oplysninger ud af en anden uden at have ret til disse oplysninger).

2.2 Forvaltning af et data brud i COPE Foundation

Der er tre elementer til styring af et databrud:

1. Oplysninger om hændelsen
2. Meddelelse om databrud og risikovurdering
3. Evaluering og respons

2.3 Hændelsesdetaljer

Oplysninger om hændelsen skal registreres nøjagtigt af DPO, herunder:

- Beskrivelse af hændelsen
- Dato og tidspunkt for hændelsen
- Dato og klokkeslæt det blev registreret
- Hvem rapporterede hændelsen og til hvem det blev rapporteret
- Typen af data involveret og hvor følsomt det er
- Antallet af personer, der er berørt af hændelsen
- Var dataene krypteret?
- Oplysninger om eventuelle involverede IT-systemer
- Bekræftende materiale

2.4 Meddelelse om databrud og risikovurdering

Intern meddelelse:

Et databrud skal omgående anmeldes af personalet til vores Systemudbyder (MultiMed A/S)

MultiMed A/S vil vurdere hændelsesoplysningerne og de involverede risici, herunder:

1. Hvilken type data er involveret?
2. Hvor følsom er de involverede data?
3. Hvor mange personers personoplysninger påvirkes af hændelsen?
4. Var der beskyttelser på plads, f.eks. kryptering?
5. Hvad er de potentielle negative konsekvenser for enkeltpersoner og hvor alvorlig eller væsentlige vil de sandsynligvis være?
6. Hvor sandsynligt er det, at negative konsekvenser vil opstå?

Ekstern meddelelse:

Hvis Speciallægepraksis BA bliver bekendt med et brud på persondatasikkerheden, skal Multimed aps uden unødig forsinkelse give besked til Datatilsynet og i visse tilfælde også til de personer, hvis oplysninger er berørt af sikkerhedsbruddet.

25-05-2018

Birgit Arentoft, gynækolog