Sikker dataopbevaring – dit ansvar

Elektroniske data – krav til sikkerhed

Opbevaring af personhenførbare data

Det er *ikke* tilladt at opbevare personhenførbare data i dokumenter eller databaser på pc'ens drev eller skrivebord.

I Region Sjælland anbefaler vi, at du får oprettet et teamsite i Sharepoint via IT-helpdesk, som er et dokumentbibliotek, der minder om stifinder i Windows. Al adgang til og brug af teamsites er logget. Det er muligt for dig at give andre Region Sjælland-medarbejdere adgang til dit teamsite vha. deres brugernavn. Læs mere om teamsites her: http://intra.regionsjaelland.dk/regionshus/praktisk/it-service/information/documents/teamsite/produktblad%20ver.3.pdf

Det er også muligt at oprette en EasyTrial licens til datahåndtering – læs mere om EasyTrial her: http://www.regionsjaelland.dk/Sundhed/forskning/forfagfolk/værktøjskasse/Documents/EasyTrial%20Sikkerhedsinformation,%20Region%20Sjælland.pdf

Endelig er det tilladt at opbevare elektroniske data på *krypteret* USB-stick eller *krypteret* harddisk – kontakt IT-helpdesk om dette. Alle udtagelige lagringsmedier (USB, eksterne harddiske mv.), sikkerhedskopier af data m.v. skal opbevares forsvarligt aflåst, så uvedkommende ikke kan få adgang til oplysningerne, når de ikke er under opsyn.

Kode- og krypteringsnøgler
Alle identifikationsoplysninger skal *krypteres eller erstattes af et kodenummer* eller lignende. Krypteringsnøglen, kodenøglen m.v. skal opbevares forsvarligt (aflåst) og adskilt fra alle personhenførbare data.

Pseudonymisering og anonymisering
Vær opmærksom på, at krypterede data eller kodede data blot er pseudonymiserede data. Data er først endeligt anonymiserede, når det ikke længere er muligt – hverken teknisk eller menneskeligt – at finde frem til den faktiske person, som data vedrører. Dette kan fx være, når krypteringsnøgle eller kodenøgle er destrueret.

Overførsel af data, fx via internet
Når du har brug for at overføre personhenførbare data via internet eller andet eksternt netværk, skal du træffe de fornødne sikkerhedsforanstaltninger mod, at oplysningerne kommer til uvedkommendes kendskab. Du skal som minimum sørge for, at data er krypteret under hele transmissionen.

Du kan læse mere om sikker e-post her:

- Digital post (e-boks*):*

  http://intra.regionsjaelland.dk/samarbejde/projekter/digitalpost/sider/default.aspx

  http://intra.regionsjaelland.dk/regionshus/aktuelt/Lokale%20nyheder%2014/Sider/Digitalposttilborgereogvirksomheder.aspx

Sikker dataopbevaring – dit ansvar

- Sikker postkasse (afdelingspostkasse):

http://intra.regionsjaelland.dk/regionshus/praktisk/it-service/it%20sikkerhed/documents/microsoft%20word%20-%20sikker%20mail.pdf

Retningslinjer for informationssikkerhed, Region Sjælland
Du kan læse mere om, hvordan du skal forholde dig i forhold til håndtering og opbevaring af data i "Retningslinjer for informationssikkerhed i Region Sjælland" (linker til intranetside)

Sikkerhedsbekendtgørelsen
Vi henviser i øvrigt til reglerne i Sikkerhedsbekendtgørelsen Nr. 528, som alle offentlige myndigheder skal overholde: https://www.retsinformation.dk/Forms/R0710.aspx?id=842

Adskillelse af data

Data i patientbehandlingssystemer

Projektets data må ikke opbevares i patientbehandlingssystemer, når der er tale om forskningsprojekter. Det er i den forbindelse vigtigt, at projektdata adskilles fra data i patientbehandlingssystemer. Der skal derfor på anmeldelsesblanketten til datatilsynet i Region Sjælland redegøres for, hvor et udtræk fra patientbehandlingssystemet opbevares under projektet.

Papirdata

Opbevaring af papirdata
Alle papirdata eller data på udtagelige lagringsmedier (USB, eksterne harddiske mv.) skal opbevares forsvarligt aflåst, når de ikke er under opsyn. Når du anmelder et projekt til Datatilsynet, er det vigtigt, at du redegør konkret for, hvor (på hvilken adresse og i hvilken afdeling) ovennævnte data opbevares inkl. rum-nr.

Biologiske data/våde data

Opbevaring af data i biobank
Hvis der benyttes biobank i forbindelse med dit projekt, er det vigtigt at sikre, at biobanken er aflåst, og at al adgang til biobanken er logget. Det skal anføres i protokollen samt i anmeldelsen til Datatilsynet, præcist hvor biobanken er lokaliseret (præcis adresse, inklusive rumnummer).

Sikker dataopbevaring – dit ansvar

Anmeldelsen til Datatilsynet

Når du anmelder et projekt til Datatilsynet i Region Sjælland, er det vigtigt, at du redegør konkret for, hvor (på hvilken adresse og i hvilken afdeling) ovennævnte data opbevares, inkl. rum-nr.

Eksempelvis:
Data opbevares i elektronisk form og papirform. Elektroniske data opbevares på krypteret USB-stick. Elektroniske data samt data i papirform opbevares på følgende adresse, i aflåst skab, i aflåst kontor: Medicinsk Afdeling, Slagelse Sygehus, Fælledvej 10, 4200 Slagelse, lokalenr.: 230-1983
Projektet benytter endvidere EasyTrial.net til opbevaring af spørgeskemadata.

Når data sendes til behandling hos ekstern part

Databehandleraftale
Hvis man som dataansvarlig benytter sig af at få data behandlet, analyseret eller opbevaret hos en ekstern part, som ikke er ansat af Region Sjælland, følger det af persondataloven, at man skal indgå en skriftlig aftale med databehandleren, en såkaldt databehandleraftale. Hertil skal endvidere fremsendes en tilhørende instruks til underskrift, der nærmere definerer databehandlerens ansvar og opgaver.
Det skal fremgå af databehandleraftalen, hvilke data databehandlingen omfatter samt hvordan de data, som databehandleren behandler, opbevares. Dette på samme vis, som de øvrige data på projektet.

Ved brug af databehandler
Det skal i denne forbindelse bemærkes, at databehandleren ikke må bruge de i forbindelse med projektet overladte oplysninger til andet end udførelsen af opgaven for den dataansvarlige.

Godkendelsen fra datatilsynet

Hvad omfatter godkendelsen fra datatilsynet?
Godkendelsen giver *alene* tilladelse til behandling af følsomme personoplysninger i et projekt til videnskabelige eller statistiske formål i henhold til persondatalovens § 10, jf. § 43, stk. 1.

Der gøres opmærksom på, at godkendelsen fra datatilsynet *ikke* omfatter tilladelse til indhentning af journaldata eller tilladelse til videregivelse af projektdata.

Du kan læse mere om indhentning af journaldata her:
http://www.regionsjaelland.dk/Sundhed/forskning/forfagfolk/projektanmeldelser/Sider/Patientjournaloplysninger-til-brug-i-forskningsprojekter.aspx

Anmodning om tilladelse til videregivelse efter persondatalovens sker ved separat ansøgning til datatilsynet. Du kan læse mere videregivelse her:
http://www.regionsjaelland.dk/Sundhed/forskning/forfagfolk/projektanmeldelser/Sider/Videregivelse%20af%20data%20fra%20tidligere%20forskningsprojekter.aspx

Sikker dataopbevaring – dit ansvar

Når projektet afsluttes

Sletning af data
Data, herunder også biologisk materiale, skal slettes, fuldstændig anonymiseres eller tilintetgøres senest ved projektets afslutning, medmindre en fortsat opbevaring kræves efter anden gældende lovgivning. Det må efterfølgende ikke være muligt at identificere enkeltpersoner i projektet.

Alternativt kan oplysningerne overføres til arkiv efter arkivlovens regler.
Link til arkivloven: https://www.retsinformation.dk/Forms/R0710.aspx?id=183862

Sletning af oplysninger fra elektroniske medier skal ske på en sådan måde, at oplysningerne ikke kan genetableres. Du kan få hjælp hos IT-helpdesk til den korrekte måde at slette elektroniske data på.

Sletningsprocedure hos en evt. databehandler
Det skal også sikres, at personhenførbare data hos databehandleren slettes, når databehandlingen jf. databehandleraftalen skal ophøre. Som projektansvarlig skal du derfor anføre tidspunkt for sletning i databehandlerinstruksen.