Sikkerhedsguide til behandlingssikkerhed af personoplysninger

Dette dokument kan bruges som en ikke-udtømmende tjekliste til, om de mest overordnede krav til sikkerhed ved behandling af personoplysninger er opfyldt:

# Vurdering af nye databehandlere / IT-systemer

* I skal foretages en vurdering af databehandlere / IT-systemer, inden de tages i brug. Vurderingen skal sikre, at databehandleren efterlever GDPR og kan tilbyde et tilstrækkeligt sikkerhedsniveau.

# Risikovurderinger

* I skal løbende gennemgå og evt. opdatere de persondataretlige risikovurderinger, som I har i klinikken. Vurderingerne afspejler de risici, som f.eks. patienter og medarbejdere udsættes for, når deres personoplysninger behandles af jer (se vejledning fra PLO).

# Fortrolighed skal sikres ved behandlingen af personoplysninger

* Kun autoriseret udstyr og relevante medarbejdere (dvs. med et arbejdsbetinget behov) må have adgang til personoplysninger. Dette kan ske ved at tildele relevante medarbejdere et unikt login/adgangsrettighed til systemet.
* Når medarbejdere fratræder, skal der lukkes for adgangsrettigheder.
* Hvis I overfører personoplysninger på det åbne internet, skal I sørge for at overførslen er sikker, evt. vha. kryptering.
* Fysisk sikkerhed (både af lokaler, adgang til computere og andre enheder samt af printede personoplysninger, såsom notater og journaler mv.)
* Låse og adgangskontroller på digitale enheder (computere, bærbare, telefoner mv.)
* Fysisk sikring af bærbare computere (f.eks. låses inde når ikke i brug eller opbevares et sikkert sted)
* Printede personoplysninger opbevares i aflåst skab (nøgle skal ikke være tilgængelig for andre)
* Kontrol med og sikring af alle flytbare medieenheder (f.eks. kryptering af USB og eksterne hardware)
* Personoplysninger fra medieenheder fjernes før udsmidning
* Personoplysninger fra harddiske på computere fjernes før udsmidning
* Sikker opbevaring af back-ups (kan sikres gennem databehandleraftale med IT-leverandør).
* Logning af adgang til IT-systemet og brugeraktivitet, herunder over fejlslagne loginforsøg og blokering af adgang ved forkert login (kan sikres gennem databehandleraftale med IT-leverandør).

# Integritet og tilgængelighed (afstemmes med IT-leverandør)

* Det skal være muligt at validere, om personoplysninger på IT-systemerne er korrekte, pålidelige, nøjagtige og fuldstændige.
* Beskyttelse af netværk, systemer, logs og personoplysninger mod manipulation udefra.
* Sikring af gendannelse af personoplysninger ved sikkerhedshændelser.

# IT-systemets robusthed (afstemmes med IT-leverandør)

* Der skal være et program for håndtering af sårbarheder i IT-systemet i forbindelse med behandling af personoplysninger. Programmet kan indeholde (men er ikke begrænset til) følgende tiltag:
  + - Undersøgelse af sårbarheden
    - Test af sårbarheden
    - Opfølgning på undersøgelser og test

# Sikkerheds- og privatlivsteknologier

* Anti-virus eller anti-malware software
* Firewall, anti-DDOS og intrusion detection

# Træning af medarbejdere

* Introduktion til medarbejdere omkring informationssikkerhed og persondatareglerne samt løbende træning

# Reaktion i forbindelse med hændelser og forretningskontinuitet

* Information om og træning af medarbejdere i forhold til brud på persondatasikkerheden og sikkerhedshændelser (f.eks. information om hvordan og hvornår sikkerhedsbrud skal anmeldes til Datatilsynet, underretning af de personer, som er omfattet af sikkerhedsbruddet, hvordan sikkerhedsbruddet håndteres, konsekvenserne mv. – se Datatilsynets vejledning om håndtering af brud på persondatasikkerheden).
* Plan for at sikre forretningskontinuitet ved alvorlig sikkerhedshændelser, f.eks. ved hacking (dette kan være f.eks. ved brug af backup).

# AUditering

* Regelmæssig kontrol af, om jeres behandling af personoplysninger opfylder kravene (f.eks. ved stikprøver af adgangskontrol, fysisk sikkerhed mv.)
* Auditering af om jeres databehandleres behandling af personoplysninger på jeres vegne opfylder kravene (skal ske løbende og dokumenteres, f.eks. én gang årligt)