Tjekliste for den it-ansvarlige i praksis

Du kan bruge tjeklisten som inspiration til, hvad du skal være opmærksom på omkring datasikkerhed i praksis.

1) **Tjek jeres backup aftale**
    a. Tages der backup af lægesystemet?
    b. Tages der backup af fællesdrevet?
    c. Hvor ofte tages der backup?
    d. Tjek regelmæssigt, at backup kan læses.
    e. Hvem har ansvaret for at sikre, at backuppen fungerer?
    f. Hvem har ansvaret for at reagere, hvis backuppen fejler?
    g. Normalt tages der ikke backup af pc'ernes skriveborde, så hvis I har data, som skal sikres, skal I gemme i de korrekte mapper – det vil sige de mapper, der tages sikkerhedskopi af.
    h. OBS spirometri og EKG: Hvis data ikke automatisk overføres til jeres journalsystem, så skal I også sikre, at der tages backup af databasen til disse eksterne programmer.

2) **Udarbejd it-politik**

Her er nogle inspirationspunkter, I kan tage udgangspunkt i:

a. It-sikkerheden årligt bliver tjekket og kontrolleret af en ekstern konsulent.
b. Alle programmer bliver jævnligt opdateret.
c. Ansatte skal lukke programmer ned ved fyraften.
d. Ansatte skal låse skærmen, når de forlader rummet (fx Windows-knappen + "L").
e. Andre kan ikke sætte en USB-nøgle i PC eller ankomstterminal.
f. Passwords bliver skiftet hver anden til tredje måned.
g. Serveren er blevet låst inde i et skab.
h. Ankomststanderen har fået en ekstra sikkerheds-plombe.
i. Private mails må ikke åbnes på arbejdscomputerne, heller ikke dadlnet-mails.
j. Sociale medier er ikke tilladt på arbejdscomputerne.
k. Google-søgninger og lign. skal foretages med varsomhed. Der må ikke søges på private emner.
l. Alle nye ansatte, også uddannelseslæger, bliver introduceret til it-sikre rutiner.
m. Aftal, hvor I må gemme statistikudtræk (fx til klyngearbejde), og hvornår det slettes.

Tjekliste for den it-ansvarlige i praksis

3) **Hvor ligger patientdata?**
   a. Hav kun patientdata i lægesystemet
   b. Hvis I modtager patientdata fra fx en hospitalsafdeling eller et forsikringsselskab via virk.dk, så sørg for at overføre data til lægesystem og slet dem i virk.dk

4) **Sørg for, at kun rette personer kan se/høre fortrolige informationer**
   a. Lås på skuffer og arkivskabe.
   b. Server skal være låst inde.
   c. Server skal være brand- og tyverisikret.
   d. Stille musik i venteværelset.
   e. Diskretionslinje ved skranken.
   f. Diskretionsseddel ved skranken (patienten skriver sit cpr.nr. i stedet for at sige det højt).
   g. Destruer papirlapper med cpr.nr. og navne.
   h. Hvordan makuleres/destrueres fortroligt materiale?

5) **Hav retningslinje for sletning af journaler**
   a. Hvordan sikrer I jer, at patientens nye læge har modtaget og indlæst journalen inden sletning?
   b. Behold journalen, hvis der er igangværende patientklage.

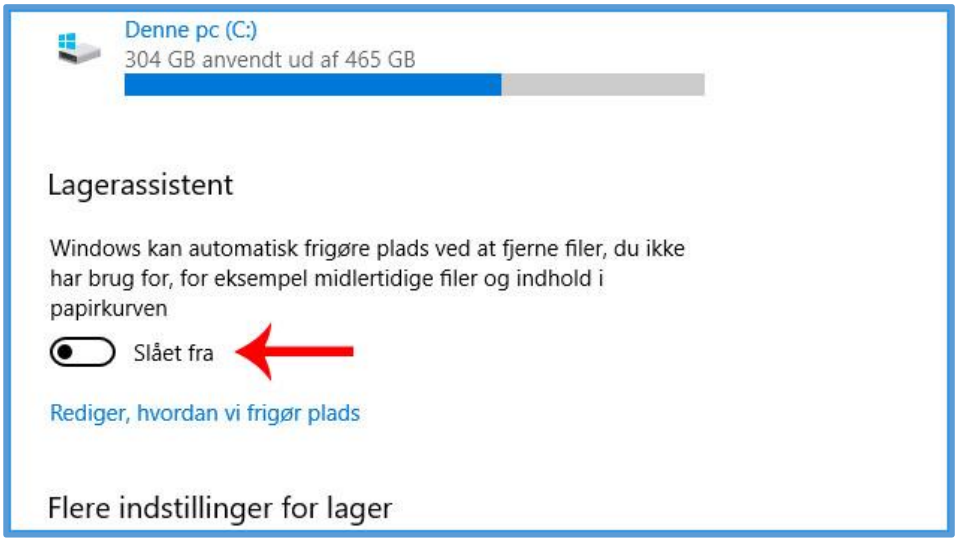
6) **Hav retningslinje for sletning af persondata på ansatte/ansøgere**
   a. Slet personoplysninger på ansatte, mulige og tidligere ansatte, når der ikke længere er brug for disse oplysninger.
   b. Hvis I ønsker at gemme en ansøgning til eventuel senere henvendelse, så husk accept fra ansøger.

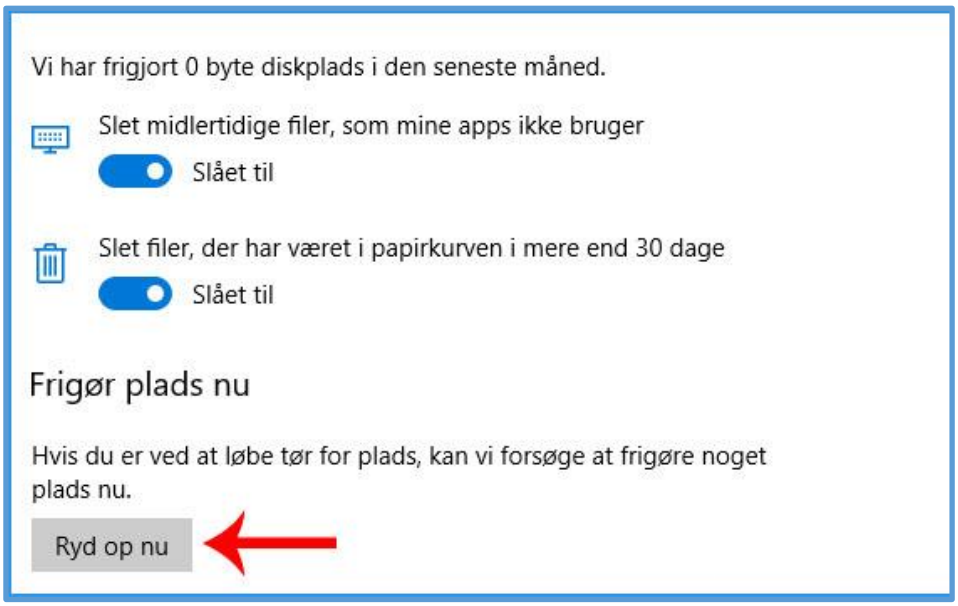
7) **Slet/inaktiver tidligere ansattes logins og adgange**
   a. Login til Windows samt lægesystem.
   b. Sundhed.dk – fjern medarbejder.
   c. Opdater MitID Erhverv.
   d. FMK-online – slet medhjælps adgange.
   e. Slet adgang til Virk.dk virksomhedens digitale postkasse (hvis de har haft adgangen).

Tjekliste for den it-ansvarlige i praksis

Forslag til hvordan I kan slette personhenførbare og følsomme informationer, som IKKE ligger i journalsystemet

a. Mulighed 1: Tøm indholdet i *Papirkurv* og mappen *Overførsler* (eller Downloads) i stifinderen.
b. Mulighed 2: Tilkobl Windows 10 lagerassistent som så automatisk laver oprydning i jeres download mappe samt papirkurven (se skærmdump nedenfor).





Hav fokus på: Fællesdrev, Dokumenter, Skrivebord, skanner, downloads

Tjekliste for den it-ansvarlige i praksis

8) Lav en retningslinje for hvad I gør, hvis I mister patientdata?

F.eks. via tyveri, nedbrud, brand, hardwarefejl eller hacking. Lav den eventuelt sammen med leverandøren af lægesystemet.

9) Hold information om praksis opdateret

a. Opdater hjemmeside.
b. Opdater infoskærm.
c. Opdater praksisdeklarationen.
d. Vedligehold information på KiAP.dk.
e. Aftal, hvem, der opdaterer praksisinformationer ved ferie/praksislukning:
    - Opdatér på sundhed.dk og praksis' hjemmeside – husk at slette info om ferie, når I er tilbage.
    - Opdatér med afløser på Fri-Ferie (> 5 dage lukkes for besked fra pt. via MinLæge app).
    - Luk evt. for e-kommunikation i lægesystemet.
    - Giv kommunen besked om ferielukning (hvis det er aftalt med jeres kommune).
f. Indlæs patientfortegnelsen hver måned (hvis lægesystemet ikke opdaterer automatisk).

10) Brug ChatGPT, apps og lignende på forsvarlig måde

a. Få en snak i praksis om, hvad I gør og må.

11) Praksis er ansvarlig for at overholde reglerne for cookies på hjemmesiden

Brugeren skal acceptere cookies til fx statistik, markedsføring og personalisering. Se PLOs vejledning.

Tjekliste for den it-ansvarlige i praksis

Nyttige links

IT-sikkerhed i almen praksis (laeger.dk)

Sådan får du en praksis, der overholder GDPR (laeger.dk)

Tjek hvor stærk dit password er

Er din email blevet hacket - er din adgangskode frit tilgængelig

https://laeger.dk/foreninger/plo/drift-af-praksis/gdpr-i-almen-praksis/sletning-af-personoplysninger

Servere i klædeskabe og ti år gamle kodeord: Ringe it-sikkerhed hos praktiserende læger | Version2

Journalføring, videregivelse: https://www.retsinformation.dk/eli/lta/2021/1225

Tjekliste for den it-ansvarlige i praksis

Du kan bestille en gratis plakat om datasikkerhed i A4-format på midtkraft.dk

Har du spørgsmål til tjeklisten, så kontakt MidtKrafts datakonsulenter. Find info på praksis.dk eller midtkraft.dk