Opbevar altid personfølsomme data på sikrede drev og husk back-up > Gem aldrig dokumenter på computerens skrivebord

Personfølsomme data dækker over patienters journaloplysninger og HR- og lønoplysninger om klinikkens medarbejdere, og med den nye persondataforordning er der kun kommet yderligere krav til, at disse oplysninger opbevares sikkert. Det kan ske på forskellige måder. Personfølsomme data kan gemmes på en server, der står i klinikken, eller det kan opbevares på en ekstern server hos et systemhus eller anden IT-leverandør.

Det vigtigste er, at der er klare aftaler om, at servere og drev er sikrede. Det vil sige, at du skal have databehandleraftaler på plads med den IT-leverandør, som tager back-up af dine data. Aftalen skal være med en klar beskrivelse af, hvor ofte der tages back-up, og hvem der har erstatningsansvar i tilfælde af tab af data mv. Det er vigtigt at sikre sine servere og drev i tilfælde af, at IT-kriminelle forsøger at hacke oplysninger, at der sker servernedbrud i klinikken, eller at klinikken skulle blive udsat for eksempelvis brand- eller vandskade.

Hvad angår opbevaring og sikring af personfølsomme data, er det også vigtigt at være opmærksom på, hvordan man bruger cloudtjenester som eksempelvis Dropbox, Icloud, Gmail eller Hotmail. Arbejdsrelaterede data bør aldrig gemmes på cloudtjenester, med mindre der er tale om erhvervsløsninger, der efterlever alle krav og regler. Brug af private cloudkonti gør det lettere for IT-kriminelle at få adgang til arbejdsrelaterede informationer og dermed personfølsomme data. Dermed øges risikoen for, at data bliver misbrugt, data går tabt eller at ondsindede vira spredes på tværs af platforme.

Tre gode råd

- Sørg for, at du har en aftale med din IT-leverandør om opbevaring og back-up af dine data. Det mest sikre er oftest, at data opbevares på en sikker server hos en professionel IT-leverandør, da IT-leverandøren har ekspertviden om opbevaring af personfølsomme data og løbende holder sig ajour med lovgivningskrav, den teknologiske udvikling og adfærd hos IT-kriminelle.

- Hvis du opbevarer data på klinikkens egen server, skal du være opmærksom på krav fra Datatilsynet til sikring af lokale serverum, hvor der opbevares personfølsomme data. Ved kontrolbesøg vil Datatilsynet bl.a. se på, om serverrummet er tilstrækkeligt sikret mod uvedkommendes adgang, at der ikke bliver opbevaret uvedkommende brandbare genstande i serverrummet, og at der ikke er øget risiko for vandskader som følge af rørføring, serverrummets beliggenhed eller indretning.

- Undgå at bruge cloudtjenester på arbejdscomputere eller andet relevant arbejdsudstyr, med mindre der er tale om godkendte erhvervsløsninger. På den måde reduceres risikoen for, at virksomhedens data bliver tilgængelige på internettet, det bliver sværere for IT-kriminelle at stjæle dataen, og det mindsker risikoen for, at Malware kan sprede sig fra private cloudkonti til virksomhedens computere og netværk.