Kom godt i gang med

Data- og informationssikkerhed på din klinik

Den stigende digitalisering er en del af tandklinikkernes hverdag. 3D røntgen og 3D scanning, fræsning af kroner og units, der kommunikerer via netværket, er blot nogle af tidens digitale tiltag. Derudover er tandlægerne på vej på sundhedsdatanettet.

I takt med den teknologiske udvikling udvider trusselsbilledet og lovgivningen sig også. Malware kan i værste tilfælde ødelægge en tandlæges forretning fuldstændig.

Desuden har EU vedtaget en ny persondataforordning, som stiller skærpede krav til klinikkernes datasikkerhed.

Plandent IT og PwC har derfor sammen udarbejdet denne folder med nogle gode råd til, hvordan du kommer i gang med at sikre din klinik.

pwc

Plandent

Beskyt dine computere

Det er vigtigt, at du behandler klinikkens computere lige så ansvarligt som alt andet udstyr på klinikken. Et nedbrud koster tid og frustrationer og kan medføre, at uvedkommende får adgang til patientdata.

Computere bør serviceres regelmæssigt og udskiftes, når de er ved at være slidte og forældede efter 3-5 år.

Det er vigtigt, at Windows og øvrig software bliver opdateret, da der løbende bliver fundet nye sårbarheder, der udnyttes til virusangreb, ransomware m.v.

Vi anbefaler, at du kun installerer software, der kommer fra klinikkens leverandører af udstyr og software. Du bør også beskytte dine computere ved at installere en anerkendt firewall og antivirussoftware.

Søg eventuelt råd og vejledning hos din IT-leverandør.

Beskyt personfølsomme oplysninger

Det er et lovkrav, at personfølsomme oplysninger skal beskyttes, så uvedkommende ikke kan tilgå disse.

Fysiske journaler og udskrifter af patientdata skal være under opsyn eller låst inde og skal opbevares i henhold til journalføringsbekendtgørelsen. Øvrige udskrifter bør makuleres forsvarligt, hvis du ikke har behov for at gemme dem.

Computere med elektronisk journalsystem og anden software indeholdende patientdata skal også beskyttes. Du skal sikre, at uvedkommende ikke kan se sundhedsoplysninger direkte på skærmen. Du bør desuden låse din computer, når du forlader den (CTRL+ALT+DELETE -> Lås computer), således at der ikke er risiko for, at andre får adgang til personfølsomme oplysninger.

Hold styr på adgang til data

Det er et krav i persondataloven, at man kan se, hvem der har tilgået hvilke patientdata, samt at uvedkommende ikke må få kendskab til disse.

Dette betyder, at hver medarbejder bør have sit eget individuelle login til journalsystemet, samt at loginoplysninger ikke deles på tværs af medarbejdere.

Det gør det muligt at foretage kontrol via journalsystemet i forhold til, hvem der har foretaget handlinger i systemet.

Luk netværket for uvedkommende

Klinikkens netværk er det første led i beskyttelsen af klinikken og skal sikres – specielt når klinikken bliver koblet på sundhedsdatanettet. Klinikkens netværk skal være beskyttet af en firewall, og kun klinikkens produktionsudstyr bør være koblet op på dette netværk (servere, computere, røntgen, units m.v.).

Tilbyder du gratis WIFI til klinikkens kunder, er det vigtigt, at dette holdes sikkerhedsmæssigt adskilt fra det øvrige netværk, således at klinikkens drift beskyttes mod evt. hacking og virusangreb via det gratis WIFI-netværk.

Det er også vigtigt at vælge en god internetudbyder. Der er meget stor forskel på kvaliteten af internetforbindelser, samt hvorvidt det er muligt at ændre indstillinger på forbindelsen. Begge dele kan have en stor betydning for, hvorledes klinikkens øvrige IT fungerer. Spørg din IT-leverandør til råds, hvis du overvejer at skifte internetudbyder.

Beskyt klinikkens server – den er livsnerven i klinikkens IT

Alle klinikkens centrale data (røntgenbilleder og journalsystemdatabase) bør være gemt på en central server. Serveren skal serviceres regelmæssigt og udskiftes, når den er ved at være slidt og forældet efter typisk 3-5 år.

Serveren bør have indbygget og opsat spejlede diske (som minimum RAID1), sådan at du ikke mister data, hvis en disk går i stykker, ligesom at serveren bør være beskyttet af en nødstrømsenhed (UPS), der også skal vedligeholdes.

Det er essentielt, at operativsystemet og softwaren på serveren holdes opdateret, således at de er beskyttede mod malware, virus og lignende, der kan true klinikkens drift og patienternes data. Der skal foretages daglig backup af serverens data.

Du bør ikke lade personer arbejde med serveren, som ikke har kendskab til dentalsoftware (røntgen, journalsystem m.v.). Det er specialiseret software med egne metodikker og opsætninger.

Arbejder du selv med serveren, bør du sætte dig grundigt ind såvel server som software, og benytter du en ekstern IT-leverandør, bør du sikre dig, at denne har erfaring med den software, du anvender på klinikken.

Fysisk indretning af klinikken

Det er vigtigt at overveje, hvordan du bedst placerer dit IT-udstyr ud fra den fysiske indretning af klinikken.

Serveren bør om muligt opbevares i et aflåst rum.

Computere bør være placerede, så uvedkommende ikke ved et uheld kan se oplysninger på skærmen.

Hvis der er personfølsomme data på datamedier (USB-diske m.v.), bør de være opbevaret således, at uvedkommende ikke kan få adgang til dem.

Husk daglig backup af data

Klinikken kan blive ramt af nedbrud og ransomware-angreb, der gør, at klinikkens data pludselig ikke længere er tilgængelige. Med en daglig backup kan klinikkens drift ofte reetableres samme dag, men uden kan du risikere at miste patientdata og journaler.

Foretager du backup til flytbare diske, bør disse være krypterede og gemmes aflåst uden for klinikken, således at de ikke forsvinder i en brand eller bliver stjålet.

Benytter du en fjernbackup-service, skal fjernbackuppen være beskyttet via eksempelvis kryptering, og den skal opbevares inden for EU. Begge dele er vigtige for at overholde persondataloven.

Vi anbefaler brug af fjernbackup-service, hvor data opbevares inden for landets grænser. En sådan service kører automatisk, og du er sikker på, at du ikke skal forholde dig til, hvorvidt dine data ulovligt udføres.

Det er vigtigt, at du flere gange årligt kontrollerer, at din backup fungerer og kan genskabes. Bruger du en IT-leverandør til din backup, skal du sikre dig, at leverandøren foretager disse kontroller. Vi har oplevet flere klinikker, der troede sig sikre, men måtte konstatere, at de havde mistet flere års data.

Pas på med at kopiere klinikkens data

Du bør som udgangspunkt ikke kopiere personfølsomme data til fx flytbare harddiske, USB-sticks og DVD'er, da der er risiko for, at kopierne kommer i hænderne på uvedkommende. Skal du kopiere data, bør de være krypterede på forsvarlig vis – sørg for at bruge en anerkendt kryptering.

Når du skifter IT-udstyr, er det vigtigt, at gamle harddiske m.v., der har indeholdt patientdata, bliver destrueret forsvarligt. Slettede data kan nemt genskabes af andre, hvis harddisken blot afskaffes på normal vis.

Send ikke følsomme oplysninger via internettet

Forsendelse af personfølsomme oplysninger til kommuner eller andre tandlæger skal ske via sikrede kanaler, da det ellers er nemt at opsnappe dine data fra internettet.

Vi anbefaler, at du benytter EDI-portalen, hvor det er muligt, da kommunikation herfra kører via det beskyttede sundhedsdatanet.

Sender du journaldata eller andre personfølsomme oplysninger via e-mail, bør disse være krypterede.

Vær også opmærksom på, at mange gratis e-mailleverandører som Hotmail og Gmail ikke lever op til de danske krav om beskyttelse af følsomme oplysninger.

Vær ikke afhængig af én nøgleperson

Der er mange klinikker, som kun har en enkelt person, der står for centrale elementer af klinikkens drift. Dette kan være en ansat eller en ekstern IT-mand, som varetager alt arbejde på serveren. Det er vigtigt, at du er forberedt på en situation, hvor vedkommende pludselig ikke længere kan udfylde denne rolle.

Vi anbefaler derfor, at du sørger for at have (korte) beskrivelser af, hvordan man:

- opretter og nedlægger brugere i IT-systemer
- vedligeholder IT-systemer, servere og netværk
- laver backup af systemer og data

Du bør også sikre dig, at du har adgang til systemerne. Du kan eksempelvis dokumentere brugernavne og passwords - og opbevare dem i en kuvert bag lås eller tilsvarende. Oftest sørger større IT-leverandører for dette, så du ikke skal bekymre dig om det.

Der er mange klinikker, hvor kun én person har kendskab til, hvorledes andre væsentlige procedurer i klinikken foregår. Vi anbefaler generelt, at du forsøger at begrænse din afhængighed af én nøgleperson for derved at begrænse dine risici.

Gennemgå risici regelmæssigt

Sikkerhed er ledelsens ansvar, og det bør sikres, at der følges op på de forskellige risici med regelmæssige intervaller. Vi anbefaler, at du mindst en gang om året afsætter tid til at foretage en vurdering af de risici, der er på klinikken generelt set, samt overvejer, om dine foranstaltninger er tilstrækkelige. Dette gælder naturligvis IT-relaterede risici, men også øvrige faktorer i relation til indbrud, brand og nedbrud på klinikkens udstyr. Samtidig bør du overveje, om du vil have en ekstern part til at foretage en gennemgang af IT-sikkerheden.

Det sker flere gange om året, at klinikker bliver alvorligt ramt af begivenheder, der skader forretningen, og som kunne være undgået.

Du kan med fordel trække på din IT-leverandør og revisor i denne sammenhæng.

Udpeg en IT-ansvarlig

Det er en stor fordel, hvis du har en medarbejder, som har det primære ansvar for klinikkens IT – uanset om du bliver serviceret af en IT-leverandør eller selv sørger for tingene.

Den IT-ansvarlige bør have overblik over klinikkens IT og skal løbende følge op på, om det fungerer optimalt. Personen bør være 'superbruger' på klinikkens journalsystem og anden software, så vedkommende kan uddanne og støtte det øvrige personale i hverdagen. Herved undgår du fejlregistreringer og andre problemer.

Den IT-ansvarlige kan med fordel tage udgangspunkt i punkterne i denne folder.

Vi hjælper dig med sikkerheden

Plandent er IT-leverandør til tandlægebranchen og er specialister i installation og integration af både hard- og software.

Plandent IT sørger for, at alt udstyr spiller optimalt sammen. Vi hjælper dig også med at finde den rette hardware til din klinik og optimerer din netværksopsætning, så alt kører stabilt og sikkert.

Vi rådgiver gerne om, hvordan du sikrer dig mod virus- og hackerangreb, og hvordan du beskytter dine data. Vi tilbyder fjernbackup-service, så du altid kan få genskabt dine patientdata.

Kontakt os på telefon 43 66 44 88 eller itsupport@plandent.dk for at høre om dine muligheder.

PwC er verdens største revisions-, skatte- og rådgivningshus. I Danmark samarbejder ca. 1.700 PwC'ere fra 15 kontorer.

Vi har specialister inden for IT-sikkerhed, som hver dag hjælper vores kunder med at sikre sig bedst muligt imod de trusler, som påvirker virksomhedernes anvendelse af digitale løsninger, sikker håndtering af kritiske forretningsdata og personoplysninger samt IT-sikkerhed generelt.

Vores ambition er at være tandlægernes foretrukne sparringspartner inden for finansielle forhold – herunder regnskabs- og skattemæssig rådgivning, driftsoptimering og forretningsudvikling.

Kontakt Allan Kamp Jensen på 40 85 88 66 eller akj@pwc.dk for at høre om dine muligheder.

Denne publikation udgør ikke og kan ikke erstatte professionel rådgivning. PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab og Plandent A/S påtager sig intet ansvar for tab, nogen måtte lide som følge af handlinger eller undladelser baseret på publikationens indhold, ligesom PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab og Plandent A/S ikke påtager sig ansvar for indholdsmæssige fejl og mangler. © 2016 PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab og Plandent A/S.