Overvejelser vedrørende datasikkerhed og tandlægejournaler

JAKOB HENNING HANSEN

I tandlægepraksis er der i dag en betydelig udfordring på sikkerhedsområdet med krav om på den ene side at følge med i udviklingen inden for teknologi og lovgivning – og samtidigt er det nødvendigt at kunne vurdere kvaliteten af de mange bud på sikkerhedsløsninger. Inden for det seneste årti har overgangen fra dokumentation på papiret til elektroniske data for alvor taget fart inden for sundhedssektoren, og tandlægefaget har taget de nye metoder til sig. Udviklingen af sundhedsdatanettet fortsætter i de kommende år med nye og omfattende løsninger på vej som eksempelvis det kommende fælles medicinkort, der udvikles til at blive brugt af hele sundhedssektoren og dermed også af tandlæger. Samtidigt med denne udvikling af de sundhedsfaglige it-systemer udvikler trusselsbilledet sig, fra de mere eller mindre "uskyldige" virusangreb, der var typiske for 10 år siden, til de mere moderne og "professionelle" forsøg på at opsnuse eller ændre bankoplysninger, CPR- og journaloplysninger med flere. Der findes i dag ikke megen hjælp at hente for den enkelte klinik, idet der ikke foreligger officielt certificerede løsninger på hverken datahåndtering eller -sikkerhed målrettet til den almindelige tandlægepraksis. De eksisterende standarder som DS 484 og ISO 17799-certificeringen, er udviklede til større virksomheder og ville være urealistisk krævende at indføre for en almindelig tandlægepraksis.

Er dine personoplysninger i sikre hænder?

Datasikkerhed vedrører alle data på en klinik med alt fra elektroniske patientjournaler, CPR og adresseoplysninger, Netbank, Dankort og Giro- transaktioner, klinikdata, personalesager til lønsystemer m.m. Den åbne og varierede brug af patientdata på klinikkerne med brug af internetbooking, mail, betaling via netbank og anden brug af internettet udgør tilsammen en kompleks, sikkerhedsmæssig udfordring for en almindelig tandlægepraksis. En stor del af disse data er tilmed udsatte for misbrug og er af interesse for uvedkommende eller kriminelle. Ifølge Danmarks Statistik (1) mistede 30 % af danske offentlige myndigheder data som følge af virusangreb, og 10 % mistede data som følge af manglende backup i løbet af 2009. Omfanget af uretmæssig adgang eller misbrug af data kan reelt være større, fordi disse hændelser ofte enten ikke anmeldes, eller simpelthen ikke opdages. I de følgende afsnit gennemgås en række af de mere almindelige risikomomenter.

Risiko 1: virus

Virus er en fællesbetegnelse for uønskede programmer eller tilføjelser på en pc med det formål at ødelægge, ændre eller få adgang til oplysninger eller andre af computerens ressourcer og netværksadgang. Virus ses i dag gemt i legitime tekst- eller videodokumenter, på USB-nøgler og andre transportable medier, hvor vira autoinstallerer uden brugerens viden eller medvirken. Generelt må en pc, der benyttes til private og uovervågede formål, betragtes som udsat, og med et netværk på klinikken med internetadgang vil alle computere være udsat på niveau med den svagest beskyttede pc i netværket.

Risiko 2: manglende backup

Problemer med backup opdages sjældent, før det er for sent, og en tandlægeklinik bør sikre sig løbende, at backuppen bliver taget, og at data kan genskabes. De fleste dataleverandører har løsninger på backup af journaldata, men alle data, der bruges på en klinik, skal kunne genskabes. Processerne bør være automatiserede, så problemer som følge af tab af patientoplysninger, fakturering, klinikadministration m.m. begrænses.

Risiko 3: uretmæssig adgang eller dataindbrud

Selv om en pc er beskyttet mod virus og fungerer i et sikkert netværk, er uretmæssig adgang eller dataindbrud mulig. Specielt transportable, trådløse netforbindelser udgør en sikkerhedsrisiko, idet de er langt mere udsatte for dataindbrud, og det er derfor vigtigt, at alle data er beskyttede og krypterede.

Et eksempel: Tandlægen forlader en ventende patient i stolen for at besvare en telefon uden at logge af hverken patientjournal eller PC. Patienten har nu fri adgang til journalerne – og ofte også til økonomi og regningssystemerne.

Et andet eksempel: En tandlæge logger ubeskyttet trådløst på klinikkens system med en laptop eller mobiltelefon, hvorved der skabes mulighed for, at andre i nærheden kan benytte samme forbindelse.

Risiko 4: hacking

Hackeraktivitet gik tidligere mest ud på at gøre opmærksom på hackernes evner til at kunne manipulere systemer, de ikke havde retmæssig adgang til. En tiltagende del af disse aktiviteter sigter i dag mod at skaffe hackeren kontrol over fx klinikkens netværk eller server til eget brug. Målet kan være alt fra lagring og distribution af ulovligt materiale til at maskere egne angreb på fremmede it-systemer eller forsøg på at få adgang til netbankkoder,

passwords, CPR oplysninger m.m.. Denne type hackeraktivitet kan være meget vanskelig at afsløre. Hvor man tidligere oplevede computeren blive langsommere, eller at den opførte sig usædvanligt: lukkede ned eller åbnede programmer eller vinduer "af sig selv", er aktiviteten i stigende grad blevet usynlig for brugeren.

Risiko 5: jagten på "den gode historie"

Ingen uvedkommende må få kendskab til klinikkens behandlinger, eller hvad den enkelte patient har fået registreret i øvrigt. Information om kendte personer kan tiltrække sig opmærksomhed eller være interessant for pressen til en "god historie". Generelt skal man derfor overveje den enkelte pc's placering; er der uovervåget adgang til computeren, eller er det muligt at følge med i, hvad der bliver skrevet.

Risiko 6: tyveri

Hvis patientoplysninger, røntgenbilleder m.m. gemmes lokalt på den enkelte klinik-pc eller på en fælles server placeret fysisk på klinikken, er der en risiko for at miste data ved tyveri eller indbrud. Hvis der er etableret en sikker og opdateret backup, mistes selve oplysningerne ikke, men tyveriet vil i sig selv udgøre en risiko for misbrug af oplysninger. Er den enkelte pc ikke adgangsbeskyttet og krypteret, vil adgangskoder, bankoplysninger og andre personoplysninger være frit tilgængelige for tyven. Misbrug af koder kan ske uden indbrud, ved simpel afluring, når koden tastes ind. Det bør sikres, at adgangskoder ikke ligger tilgængelige i skuffer, på opslagtavler eller helt åbenlyst sidder på en gul, selvklæbende seddel ved siden af skærmen.

Risiko 7: tekniske problemer

It-udstyr har en begrænset holdbarhed; en almindelig pc forventes således at have en holdbarhed på 3-5 år (2). En del udstyr er ikke robust og tåler ikke simpel rengøring, støvsugning, varme eller fugt. Det må derfor anbefales at udskifte harddiske m.m. i god tid og ikke vente til udstyret "ikke kan mere". Servere stiller særlige krav til mekanisk sikkerhed, brandsikring, alternativ strømforsyning (UPS) m.m., og for mindre klinikker vil det sjældent kunne svare sig selv at stå for serverdrift og vedligehold.

Risiko 8: mangelfuld uddannelse

Uddannelsen af den enkelte medarbejder er en væsentlig forudsætning for at minimere fejlbetjening eller fejlregistrering i journalerne, og instruktion af medarbejdere er tillige lovpligtig (3). Der bør i instruktionen ikke blot lægges vægt på indøvelse af de mest almindelige arbejdsgange, men også gives en forståelse for vigtigheden af viden om systemerne og deres sikkerhed.

Risiko 9: leverandørerne

En useriøs leverandør vil let kunne kompromittere sikkerheden ved at bruge uautoriseret software, billige usikre hardwareløsninger eller ved at håndtere bl.a. backupløsninger forkert. Eksempler fra forfatterens egen erfaring: En dataleverandør glemte simpelthen at skifte båndet til en backup, når det var fuldt - og dermed blev der reelt ikke taget backup i flere måneder for en større medlemsorganisation. Et andet eksempel er en leverandør, der på grund af ferie eller sygdom simpelthen sparer de procedurer væk, som kunderne ikke umiddelbart lægger mærke til i det daglige.

Mange firmaer er dog seriøse og leverer gennemførte datasystemer til tandlægeklinikker med både totalløsninger og mere specialiserede kliniksystemer med journalsystemer, røntgensy-

stemer, klinikadministration mv. Der er hen ad vejen dannet en de facto kvalitetsstandard, udformet af de mest udbredte leverandører til praksis, men der findes ikke en officiel godkendelse. Eneste undtagelse er, at tandlægers regningsforsendelser via Sundhedsdatanettet kræver, at MEDCOM-standarden er opfyldt, og på dette punkt foreligger en test af tandlægesystemernes opfyldelse af standarderne (5). Samlet mangler der aktuelt en praktisk og fagligt målrettet certificering af leverandører til tandlægepraksis til støtte for den enkelte kliniks valg af leverandør og softwareløsninger. Udviklingen af sundhedsdatanettet kan dog ændre dette billede i fremtiden, når tandlægeområdet for alvor kommer med i et fælles, elektronisk medicinkort, og når e-journalerne bliver udbredt til hele sundhedsvæsenet.

Risiko 10: fejlhåndtering og privat anvendelse af it

Fejl i betjening eller brug af data kan opstå i mange situationer: fra at efterlade en pc med journalen åben og ubeskyttet til fejlskrivninger, uretmæssig udlevering af data eller passwords m.fl. Fejl kan ikke udelukkes selv i meget sikre systemer og med velinstrueret personale. Det er derfor vigtigt, at alle handlinger logges automatisk. En pc, der håndterer patientjournaler, regninger eller klinikadministration, bør som minimum sikres med adgangsbeskyttelse (6); download, kopiering eller anden brug af private filer bør ikke finde sted på samme pc.

I tilfælde hvor der er sket fejl i patientbehandlingen eller i klagesager, kan en behandler måtte ønske at skjule fejl ved illegitimt at ændre i journalen og andre steder, men logges brugerens adfærd, vil der være større sandsynlighed for, at en sådan handling bliver opdaget. Tilskyndelsen til at foretage ulovlige ændringer i patientjournalen vil være tilsvarende mindre.

Risiko 11: oplysninger sendt via internet

Så snart data sendes – uanset forsendelsesmetoden – vil der være en risiko for, at oplysningerne havner i de forkerte hænder eller bliver ændrede (3). Der er ingen tvivl om, at ikke sikrede hjemmesider kan udgøre en risiko, og der er derfor også krav om kryptering. Der foreligger ikke dokumentation for, at e-mail i øvrigt skulle udgøre en større risiko for, at data havner forkerte steder, end almindelig brevpost (7). Det er alligevel ikke tilladt ifølge persondataloven at sende fx CPR-oplysninger eller andre personhenførbare data via mail uden stærk kryptering (8).

Risiko 12: personaleskift

Når klinikpersonale holder op på klinikken, er det vigtigt, at adgangskoder lukkes, men også at klinikken har en fast procedure, som sikrer, at data, som denne person har haft adgang til, stadig er tilgængelige. Det vigtige er, at sådanne retningslinjer foreligger ved ansættelsen og ikke skal "opfindes" ved ansættelsens ophør. Et særligt tilfælde af dette er ved klinikoverdragelse, sygdom eller død. Det er i Danmark lovpligtigt at sikre, at journaloplysningerne kan gives videre til patienten eller til den tandlæge, der overtager praksis (9). Data og backup skal være opbevaret sikkert, men samtidigt tilgængelige; eksempelvis, at nøgler eller adgangskoder opbevares i pengeskab, eller hos advokat evt. sammen med testamente med videre.

Risiko 13: for meget af en god ting; for høj sikkerhed

Et meget højt og dermed tidskrævende sikkerhedsniveau for brugerne kan indirekte føre til en sikkerhedsbrist, hvis sikkerhedsprocedurerne opleves af brugerne som et dagligt irritationsmoment, der er besværligt eller forsinkende i det daglige arbejde. Det kan resultere i en "afværgeadfærd" hos personalet: Compu-

teren lukkes fx ikke ned, eller brugeren logger ikke af efter endt brug, alle anvender samme log ind, en klinikassistent tænder og logger ind om morgenen til alle. Kreativiteten kan være forbløffende stor i en travl hverdag med stor og berettiget vægt på det kliniske arbejde.

Det er derfor vigtigt løbende at motivere og inddrage medarbejderne i de konkrete sikkerhedsprocedurer og mindst lige så vigtigt at afstemme sikkerhedsniveauet i forhold til det påkrævede og nødvendige.

Generelle sikkerhedsråd til en tandlægepraksis

Leverandørerne af dentalsystemer stiller ofte specifikke krav til opsætning af klinikkens it. Det må naturligvis anbefales at følge den konkrete leverandørs anvisninger, og de følgende generelle råd er skrevet med dette forbehold, men det er almindeligt, at leverandørerne frasiger sig ansvaret for både sikkerhedsinstallationen og tredjepartsprodukter, så i den sidste ende er det alene klinikejerens ansvar at kravene til sikkerhed er opfyldt. Konkrete anvisninger på egnede leverandører eller gode løsninger er uden for denne artikels rammer.

Uanset om man vælger en totalløsning hos en af de specialiserede leverandører med alt fra hardware til support og backup, sikkerhedsopdateringer og journal- og økonomisystem, eller om man vælger at varetage dele af opgaven selv, så bør klinikken udpege en sikkerhedsansvarlig, som har adgang til alle oplysninger i systemet, holder sig opdateret på området, og som vil påtage sig at instruere det øvrige personale i arbejdsgangene.

Fysisk sikkerhed

Der skal træffes sikkerhedsforanstaltninger, der sikrer mod tyveri, hærværk og uvedkommendes adgang. Dette vil ofte være på

plads på en tandlægeklinik, men opbevares backup harddiske mv. uden for klinikken, er det vigtigt, at de er sikrede tilstrækkeligt i pengeskab eller lignende.

Pc til privat anvendelse på klinikken

Hvis klinikken tillader, at en klinik-pc anvendes til privat brug, skal der fastsættes retningslinjer for brug. Det anbefales enten at installere en hardwarebaseret separationsboks til to selvstændige harddiske, eller alternativt blot at anskaffe en dedikeret pc, som ikke bruges af klinikken til patientregistreringer. Herved vil den private anvendelse adskilles fra den rent arbejdsmæssige brug.

Internet og mail

Som udgangspunkt er alle personoplysninger følsomme og skal være beskyttet af en stærk kryptering, hvis de transmitteres via mail eller internet. Der findes officiel kodning som MEDCOM beregnet til transmission via sundhedsdatanettet, og der findes et udvalg af tilgængelige krypteringsmetoder til mailbeskyttelse, som fx PGP, OpenPGP eller GnuPG. Alternativet er at undlade personhenføre data i mailen ved at fjerne de sidste cifre i CPR-nr. eller lignende og på anden måde sikre identifikationen. Personrelaterede oplysninger må aldrig udveksles på ikke sikre hjemmesider, eller sendes i form af PDF-filer, PowerPoints, skærmbilleder eller lignende uden kryptering. Hjemmesider med SSL-krypering betragtes som sikre og kan benyttes. Afsenders/modtagers identitet og de transmitterede oplysningers ægthed skal sikres med fx elektronisk signatur eller individuelle, fortrolige adgangskoder (3,9). Det anbefales også at foretage kryptering, hvis andre fortrolige oplysninger som eksempel oplysninger om økonomiske forhold mv. sendes via mail eller web.

Firewall

Datatilsynet angiver, at personoplysninger altid som minimum beskyttes ved opsætning af en Firewall, og at denne vedligeholdes løbende (8) for at beskytte klinikken mod udefrakommende hackerangreb. Leverandører af dentalsystemer kan stille specifikke krav til Firewall-installationen, antivirusprogram eller internetsikkerhed i forbindelse med journaler, fjernsupport og backupløsninger med automatiseret dataudveksling. På mindre klinikker og pc'er til privat anvendelse kan Windows indbyggede Sikkerhedscenter hjælpe til at få overblik over firewall, automatiske opdateringer, antivirus- og spywareprogrammer og andre sikkerhedsindstillinger.

Antivirusprogrammer mv.

Et vedligeholdt antivirusprogram er absolut nødvendigt. Enkelte leverandører af dentalsystemer udpeger foretrukne produkter, og det må generelt anbefales at følge disse vejledninger.

Automatiske opdateringer

Der findes flere programmer i handlen, som automatisk kan holde de programmer, der ligger på en pc, opdaterede og advare om sikkerhedsrisici. Ved Microsoft produkter bør opdateringerne fra Microsoft update sættes til "automatisk" på alle computere.

Adgangsbeskyttelse

Adgangsbeskyttelse med brugernavn og kode er vigtig, så kun godkendte personer kan få adgang til journaler m.m. Adgangsbeskyttelsen er lovpligtig (6) og de almindelige styresystemer giver sådanne muligheder. Elektroniske journalsystemer har indbygget brugerstyring, men er undertiden blot et simpelt valg af bruger uden password og udgør dermed ingen tilstrækkelig

sikkerhed for brugeridentitet. Adgangsbeskyttelse er ofte et kompromis imellem brugervenlighed og sikkerhed, men systemer uden en sådan beskyttelse bør aldrig anvendes.

Brugerkontrol

Brugerkontrol er lovpligtig (8) og giver styr på, hvad der installeres eller ændres på den enkelte pc. Windows 7 har mulighed for individuelle rapporter for hver enkelt brugerkonto, men dette kan medføre, at visse journalsystemers egen brugerstyring ikke fungerer. Tillader dentalsystemet disse rapporter, må det anbefales at bruge dem. Det er vigtigt at gennemgå arbejdsgangene og begrundelserne med klinikpersonalet grundigt inden indførelse af brugerkontrol, idet dette ellers kan være en "sten i skoen" i samarbejdet på klinikken.

Backup

Det anbefales at samle alle data på en server; hvis dataleverandøren ikke tilbyder dette, eller det foretrækkes, kan Windows Server automatisere processen, så serveren automatisk sikkerhedskopierer alle computere på netværket. Manuel sikkerhedskopiering på hver enkelt computer anbefales ikke generelt.

Vedligeholdelse

Det bør være rutine at rense hardware og opdatere og scanne for virus med faste mellemrum, mindst en gang ugentligt.

Reparation, salg og kassation

Det er vigtigt at sikre mod misbrug af data i tilfælde af reparation og service. For eksempel vil indlevering af harddisken til reparation kunne udgøre en ulovlig videregivelse af oplysninger. Ved kassation af lagringsmedier og øvrigt udstyr, som indeholder

personoplysninger, bør lagringsmedierne destrueres eller afmagnetiseres, så der ikke er mulighed for at læse indholdet. Hvis lagringsmedier afhændes med henblik på genbrug, skal de lagrede oplysninger slettes effektivt. Overskrivning eller "sletning" er ikke tilstrækkelig; antivirussystempakker har ofte funktioner, der kan slette data sikkert, og disse bør anvendes i stedet.

Følg med

Interne sikkerhedsbestemmelser på en klinik skal gennemgås og ajourføres mindst en gang årligt (8). På grund af udviklingen er det afgørende vigtigt, at den it-ansvarlige på klinikken holder sig opdateret. De seriøse dataleverandører har informationstjenester til formålet, og generelle oplysninger kan i øvrigt findes ved at abonnere på Datatilsynets nyhedstjeneste (www.datatilsynet.dk). Oplysninger vedrørende virus eller andre trusler kan findes på bl.a. flere af antivirus-leverandørers informationshjemmesider.

LITTERATUR

1. Danmarks Statistik. Den offentlige sektors brug af it 2009; 2010.
2. Miljøstyrelsen. Miljøvejledning for kontorelektronik; 2005.
3. Retsinformation: Vejledning til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. www.retsinformation.dk
4. MedCom. MedCom – det danske sundhedsdatanet. www.medcom.dk
5. MedCom. Tandlægesystemer Afsender og modtagertest. www.medcom.dk
6. Datatilsynet. Datatilsynets sikkerhedsbekendtgørelse: Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. BEK nr. 528 af 15/06/2000.
7. Datatilsynet. Oversigt over høringssvar i forbindelse med Datatilsynets sag om sikkerhedskrav ved transmission af personoplysninger via internettet i den private sektor. 2007. www.datatilsynet.dk
8. Datatilsynet. Vejledning nr. 37 af 2. april 2001 www.retsinformation.dk
9. Retsinformation. Bekendtgørelse om lægers, tandlægers, kiropraktorers, jordemødres, kliniske diætisters, kliniske tandteknikeres, tandplejeres, optikeres og kontaktlinseoptikeres patientjournaler (journalføring, opbevaring, videregivelse og overdragelse m.v.) BEK nr. 1373 af 12/12/2006