Informationssikkerhed i din klinik

En vejledning for praktiserende læger

PRAKTISERENDE LÆGERS ORGANISATION

PRAKTISERENDE
LÆGERS
ORGANISATION

Om publikationen

”Informationssikkerhed i din klinik” indeholder råd og vejledning om, hvordan du som praktiserende læge kan beskytte de oplysninger, du arbejder med, og hvordan du bedst muligt sikrer dig, at dine fysiske og digitale informationssystemer fungerer tilfredsstillende. Publikationen indeholder desuden en række praktiske råd om, hvorledes du sikrer data, og lever op til lovgivningen samt god IT-skik.

De IT-trusler, vi udsættes for, er i konstant forandring, og det samme er de procedurer og værktøjer, vi alle skal benytte for at beskytte os. Derfor bør vejledningen opfattes som et dynamisk dokument. Vejledningen vil senere i 2017 blive tilbudt i en elektronisk version, der jævnligt vil blive opdateret.

Publikationen giver dig ikke svar på alle spørgsmål, og den er ikke nødvendigvis udtømmende i forhold til, hvordan du kan sikre en tilstrækkelig informationssikkerhed i din klinik i alle henseender. Betragt publikationen som en række gode råd og praktisk vejledning. Vil du vide mere, kan du med fordel orientere dig i litteraturlisten på side 12 i publikationen.

”Informationssikkerhed i din klinik” er udviklet af Praktiserende Lægers Organisation med udgangspunkt i Sundhedsdatastyrelsens ”Vejledning om informationssikkerhed i sundhedsvæsenet”, og med kompetent bistand fra styrelsens personale. Også MedCom og Primærsektorens Leverandørforum har bistået med gode råd og anvisninger. Tak til alle bidragydere for værdifuld viden og vejledning.

Christian Freitag
Formand for Praktiserende Lægers Organisation

MARTS 2017

Indhold

Ejeren eller de ansatte i den enkelte praksis kan blive stillet til ansvar, hvis informationssikkerheden er kompromitteret.

FOTO: LARS JUST

Formål

Det danske sundhedsvæsen består af en lang kæde af aktører, og igennem den kæde flyder informationer, som er vitale for alle involverede. De praktiserende læger er en vigtig del af den kæde.

En kæde er imidlertid aldrig stærkere end sit svageste led, og derfor er det afgørende for informationssikkerheden i sundhedsvæsenet, at alle aktører bidrager til at behandle alle væsentlige informationer med passende omhu.

Formålet med "Informationssikkerhed i din klinik" er at tilbyde den praktiserende læge og klinikkens øvrige personale en guide og et praktisk værktøj, der kan medvirke til at forebygge og kontrollere sikkerheden for de informationer, som vedrører din klinik og dine patienter. Det vil derfor være en god idé, hvis både du og dine ansatte har et godt kendskab til indholdet i vejledningen.

Følger du anvisningerne kan du inden for rimelige økonomiske rammer leve op til god IT-skik. Samtidig vil du have nogle redskaber, som med en lille indsats vil gardere dig imod sikkerhedssvigt. Du vil derudover leve op til lovgivningens krav om ansvarlig IT-drift.

"At drive en effektiv praksis i tæt samarbejde med det omgivende sundhedsvæsen og patienterne kræver, at informationsteknologi bruges aktivt. IT er også en forudsætning for, at praksis kan arbejde med databaseret kvalitetsudvikling og have adgang til opdateret faglig viden og beslutningsstøtte. IT skal bruges stadig mere aktivt i almen praksis og kommunikation med patienter og det øvrige sundhedsvæsen, og nye teknologiske muligheder tages løbende i brug".

(Overenskomst om almen praksis)

Informationssikkerhed generelt

Informationssikkerhed er en bred betegnelse som både bruges ved akkreditering og certificering. Betegnelsen dækker over IT-sikkerhed, men den dækker også over sikkerhed omkring papirbårne dokumenter, vejledninger, og administrative dokumenter såsom kontrakter med leverandører samt ansættelseskontrakter. Denne pjece har hovedsageligt fokus på IT-sikkerhed, men du skal være opmærksom på, at det er din pligt at udvise samme omhyggelighed på hele paletten.

Ti gode grundregler

1. Brug professionelt programmel imod ondsindede programmer og vær sikker på, at det løbende opdateres.
2. Hold dine programmer, styresystemer og apps opdaterede.
3. Undgå skadelige downloads, når du besøger hjemmesider. Undlad brug af din PC til andet end arbejdsrelaterede opgaver. Tjek sikkerhedsniveauet i din browser.
4. Såfremt der findes trådløse netværk (WiFi) på klinikken, bør dette adskilles fra klinikkens arbejdsnetværk, så der ikke er forbindelse mellem de to netværk. Risikoen for en evt. "bagdør"/trojansk hest fra mobiltelefoner og andet it-udstyr er særdeles stor. Et WiFi netværk skal altid sikres med minimum WPA2 kryptering, og koden bør udskiftes med jævne mellemrum.
5. Åbn ikke links eller filer i e-mail, du får sendt uopfordret.
6. Brug adgangskoder med minimum 8 karakterer indeholdende tal, tegn og bogstaver.
7. Tag daglig sikkerhedskopier af dine data og kontroller, at sikkerhedskopien kan læses ind.
8. Undlad at indtaste personlige data på hjemmesider, du ikke kender.
9. Tilkobl aldrig USB-nøgler, cd'ere og transportable harddiske, du ikke kender.
10. Pas på dit nøglekort og din kode til NemID. De må kun anvendes af dig personligt, og kode samt nøglekort må aldrig opbevares sammen.

Kort om lovgivningen

Informationssystemer er vitale for enhver moderne lægepraksis. Derfor bør den praktiserende læge have en politik for sin informationssikkerhed, eller i det mindste have gjort sig grundige overvejelser på området. Disse overvejelser bør udmøntes i procedurer, der sikrer fortrolighed, sammenhæng og adgang til klinikkens informationssystemer.

Retningslinjerne skal tage udgangspunkt i lovgivningen, men tilpasses de tekniske og praktiske forhold i din klinik. Især to love er meget relevante.

A. **Sundhedsloven** regulerer bl.a. sundhedspersoners videregivelse og indhentning af personoplysninger i behandlingssammenhænge. Loven præciserer, hvem der må få adgang til data, der er registreret i forbindelse med behandlingen i f.eks. elektroniske patientjournaler, laboratoriesystemer og systemer i lægepraksis. Bemærk, at lovens kapitel 9 supplerer de generelle regler i persondataloven.

B. **Persondataloven** er den lov, der implementerer EU's databeskyttelsesdirektiv i dansk lovgivning. Men er der regler i anden lovgivning, der giver borgerne en bedre retsstilling, er det disse regler, som gælder. Et eksempel er netop det omtalte kapitel 9 i sundhedsloven. Dette kapitel fastlægger betingelserne for adgangen til personoplysninger i forbindelse med behandling af patienter, og her er reglerne mere specifikke i forhold til persondataloven.

I persondataloven skelnes der mellem

1. *Almindelige personoplysninger,* som f.eks. kan være oplysninger om identitet og økonomiske forhold (persondatalovens § 6).
2. *Følsomme oplysninger,* der omfatter oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbred og seksuelle forhold.

Loven er opdelt sådan, fordi der stilles andre krav til behandling af følsomme oplysninger, f.eks. om, hvem der må få adgang til oplysningerne samt til de tekniske og organisatoriske tiltag, der skal gøres, for at beskytte oplysningerne.

Almen praksis er omfattet af både sundhedsloven og persondataloven, uanset om informationerne befinder sig på papir eller elektronisk. Det betyder, at ejeren eller de ansatte i den enkelte praksis kan blive stillet til ansvar, hvis informationssikkerheden er kompromitteret, eller hvis en person lider tab eller skade på grund af misbrug af information i almen praksis.

Der er vedtaget en ny EU-persondataforordning, der får virkning i Danmark fra 25. maj 2018, og som skærper kravene på en række punkter og strammer strafbestemmelserne for at beskytte borgernes privatliv. Kravene vil blive nærmere beskrevet, når EU-forordningen er implementeret i dansk lov. PLO arbejder med at sikre ensartede, veludviklede løsninger, som betyder, at alle praktiserende læger kan tilbyde deres patienter en oversigt over hvilke data, der anvendes i klinikken, hvem disse data deles med, til hvilke formål m.v.

Se også oversigten over centrale love og bekendtgørelser i litteraturlisten side 12.

Behandling af data

Vurdering af risiko
Inden du går i gang med at udbygge eller forbedre din informationssikkerhed, bør du foretage en risikovurdering. Niveauet for sikkerheden i din klinik bør altid ske ud fra en afvejning af arbejdsopgaver, økonomi og risici. Hvilke trusler er de mest sandsynlige, hvilke kan gøre størst skade, og hvor skal du prioritere din indsats? På den måde får du mulighed for at afveje din indsats.

Patientens data er "need to know"
Det ligger dybt i enhver praktiserende læges bevidsthed, at informationer om de enkelte patienter skal behandles med den største omhu. Tilsvarende har patienterne også en forventning om, at alle informationer, der udveksles mellem dem og deres læge, bliver holdt fortrolige.

Derfor skal den praktiserende læge og øvrigt personale i klinikken som udgangspunkt kun behandle data om deres patienter, når det er påkrævet. For almen praksis er der især tre situationer, hvor lægen og klinikkens medarbejdere behandler personlige data om patienter:

1. Når den enkelte patient er i behandling
2. I forbindelse med faglige diskussioner internt i klinikken
3. I forbindelse med honorarafregning med Sygesikringen

Derudover kan helbredsoplysninger anvendes til videnskabelige og statistiske undersøgelser. Hvis du deltager i en undersøgelse med brug af patientoplysninger fra dit lægepraksissystem, kan du læse mere på side 7 nederst.

Beskyttelse af patientoplysninger
Som udgangspunkt skal den praktiserende læge eller klinikkens personale registrere alle oplysninger, der er relevante for patientens behandling.

Som udgangspunkt skal den praktiserende læge kun behandle data om deres patienter, når de er i behandling.

FOTO: LARS JUST

Ifølge persondataloven er du som praktiserende læge *dataansvarlig*, når du behandler patientoplysninger. Også her er du underlagt persondatalovens krav om at etablere tilstrækkeligt tekniske og organisatoriske foranstaltninger til at beskytte oplysningerne. På det offentlige område gælder den såkaldte Sikkerhedsbekendtgørelse med beskrivelse af en række sikkerhedsforanstaltninger, som almen praksis også bør leve op til.

Den praktiserende læge lader, som dataansvarlig, ofte en ekstern part, en databehandler, udføre den praktiske behandling af personoplysninger. Den eksterne part kan f.eks. være en leverandør, der drifter dine it-systemer. Leverandøren må kun behandle patientoplysninger ud fra de instrukser, han har modtaget fra dig som dataansvarlig, i en skriftlig aftale, en databehandleraftale. Af aftalen fremgår det bl.a., hvilke opgaver der skal løses, og hvilke sikkerhedsforanstaltninger, som leverandøren skal have på plads.

I forbindelse med den kommende EU-persondataforordning ønsker PLO, at alle klinikker kommer til at operere under en ensartet databehandleraftale.

Hvis klinikken anvender eksterne konsulenter til udvikling eller support af sine IT-systemer, og hvis konsulenterne derved får adgang til patientoplysninger, bør klinikken også indgå en aftale med disse konsulenter.

Takket være de teknologiske muligheder opsamler borgerne på eget initiativ i stigende grad oplysninger om deres helbred i apps på f.eks. deres mobiltelefon eller ved hjælp af andre løsninger. Disse oplysninger er ikke patientoplysninger. Det bliver de først, hvis du som læge inddrager dem i behandlingen af patienten og lægger dem ind i praksisjournalen. Så træder sundhedsloven og persondataloven m.v. i kraft.

Patientens adgang til egne oplysninger
Alle patienter over 15 år har ret til at få aktindsigt i de registrerede oplysninger, hvis de er journalført efter 1. januar 2010. Kravet om aktindsigt gælder for så vidt også før den dato, men her kan aktindsigten begrænses, hvis der er afgørende hensyn, der skal tages til patienten selv eller andre private interesser.

Anmoder en af dine patienter om aktindsigt, skal du efterkomme anmodningen inden for syv arbejdsdage. Patienten har krav på at se alle de oplysninger, du har registreret om vedkommende samt de oplysninger, der stammer fra sygehuse eller speciallæger.

Patienters adgang til aktindsigt i deres patientjournal er beskrevet i sundhedslovens kapitel 8.

Når du skal dele oplysninger om dine patienter
En høj lægefaglighed forudsætter, at læger og sundhedspersonale har mulighed for at dele viden med hinanden. Aktiv anvendelse af oplysninger fra patientjournaler baner i mange sammenhænge vejen for en bedre behandling af patienterne. Men oplysningerne kan også misbruges, og derfor sætter lovgivningen også grænser for anvendelse af patientdata.

Af persondataloven og sundhedsloven fremgår det, at man som udgangspunkt kun må videregive oplysninger til andre, hvis man har samtykke fra den person, oplysningerne vedrører. Men i praksis kan lægen videregive oplysninger uden et konkret samtykke, når det f.eks. drejer sig om oplysninger, der er nødvendige for den aktuelle behandling af patienten. Husk, at kun oplysninger, der er nødvendige for den aktuelle behandling, må videregives.

Når det drejer sig om at indhente oplysninger, kan den praktiserende læge indhente både historiske og aktuelle oplysninger om patienten på tværs af sektorer og behandlingsenheder, når det drejer sig om patienter, der aktuelt er i behandling. Klinikkens personale må kun hente historiske oplysninger, hvis de bliver bemyndiget til det af den praktiserende læge. Denne bemyndigelse skal være skriftlig, så den kan udleveres til patienterne, hvis de beder om den.

Sørg for, at kun personer, der er relevante for patientbehandlingen, arbejder med de konkrete data om patienten. Bemærk også, at det på ingen måde er lovligt at søge oplysninger om patienter, der er tilknyttet en anden behandlingsenhed, f.eks. en anden almen praksis.

Derudover kan – og i nogle tilfælde *skal* - almen praksis videregive patientoplysninger, hvis de har almen samfundsmæssig betydning. Det kan f.eks. være til forskning eller statistik, hvis patienten har en særlig smitsom sygdom, hvis oplysningerne har betydning for en offentlig myndigheds sagsbehandling, eksempelvis ved dødsfald, og ved indberetning til regionale eller landsdækkende kvalitetsdatabaser, der overvåger behandlingsresultater. En række af disse særlige tilfælde er reguleret i sundhedslovens § 43 og § 44.

Oplysninger, der ikke er dækket af de nævnte undtagelser, må kun videregives, hvis patienten har givet sit samtykke. Husk at indføre samtykket i journalen.

Den praktiserende læge skal sikre, at klinikkens personale og tekniske udstyr er i stand til at kommunikere personoplysninger på nettet sikkert og forsvarligt.

PLO har udarbejdet syv principper om praktiserende lægers adgang til deling af journaloplysninger. Du kan finde linket til principperne i litteraturlisten på side 12.

Ansvar og pligter
Alle medarbejdere i almen praksis, der arbejder med fortrolige data, har *ansvaret* for, at

- klinikkens informationer kun er tilgængelige for de medarbejdere, der har tilladelse til at anvende informationerne
- uvedkommende ikke får kendskab til eller viden om fortrolige informationer

Alle medarbejdere i klinikken, der arbejder med kvaliteten af data, er *forpligtet* til at

- være omhyggelig med, hvilke data, der tilgår klinikkens informationssystemer
- kontrollere, at den korrekte patientjournal er på skærmbilledet, før journalen opdateres
- have kendskab til, hvordan systemerne skal anvendes, og hvorledes de skal opdateres, så de virker efter hensigten
- rapportere alvorlige fejl i informationssystemerne til den person i klinikken, der har ansvaret for informationssikkerheden

Alle klinikkens medarbejdere og samarbejdspartnere skal være bevidste om deres personlige ansvar. Derfor skal

- klinikkens regler for fortrolighed indgå som en del af ansættelseskontrakten
- den enkeltes ansvar for sikkerheden være en del af vedkommendes jobbeskrivelse
- kontrakter med leverandører have passende klausuler om sikkerhed og fortrolighed

Sikkerhed på nettet

Det stadig tættere samarbejde mellem parterne i sundhedsvæsenet betyder, at der udveksles stadig flere fortrolige og følsomme oplysninger på tværs af organisationer og personer.

Af persondataloven fremgår det klart, at den dataansvarlige, f.eks. den praktiserende læge, skal sikre, at klinikkens personale og tekniske udstyr er i stand til at kommunikere personoplysninger på nettet sikkert og forsvarligt. Eller sagt med andre ord: Under transmissionen på nettet må oplysninger ikke blive forringet, de må ikke gå tabt, og de må ikke kunne misbruges.

I praksis kan det være svært for almindelige IT-brugere at vurdere, om et netværk er sikkert – altså om det er "åbent" eller "lukket". Det skyldes ikke mindst, at mange brugere i dag arbejder i trådløse netværk, og at de netværk også er forbundet med andre netværk hos samarbejdspartnere.

Lad dig ikke narre

Svindlere forsøger i stigende grad at franarre os fortrolige data. De sender en mail med et link, der foregiver at være din bank eller en offentlig myndighed. Hvis du klikker på linket og indtaster oplysninger, ender de hos svindlerne. Derfor skal du altid sikre dig, at domænet er korrekt, f.eks. www.datatilsynet.dk og ikke www.dk-datatilsynett. Tjek også om websiden krypterer dine oplysninger, hvilket den gør, når webadressen begynder med "https" i stedet for "http". Som udgangspunkt vil offentlige myndigheder i øvrigt aldrig sende dig mails med links, som du skal klikke på.

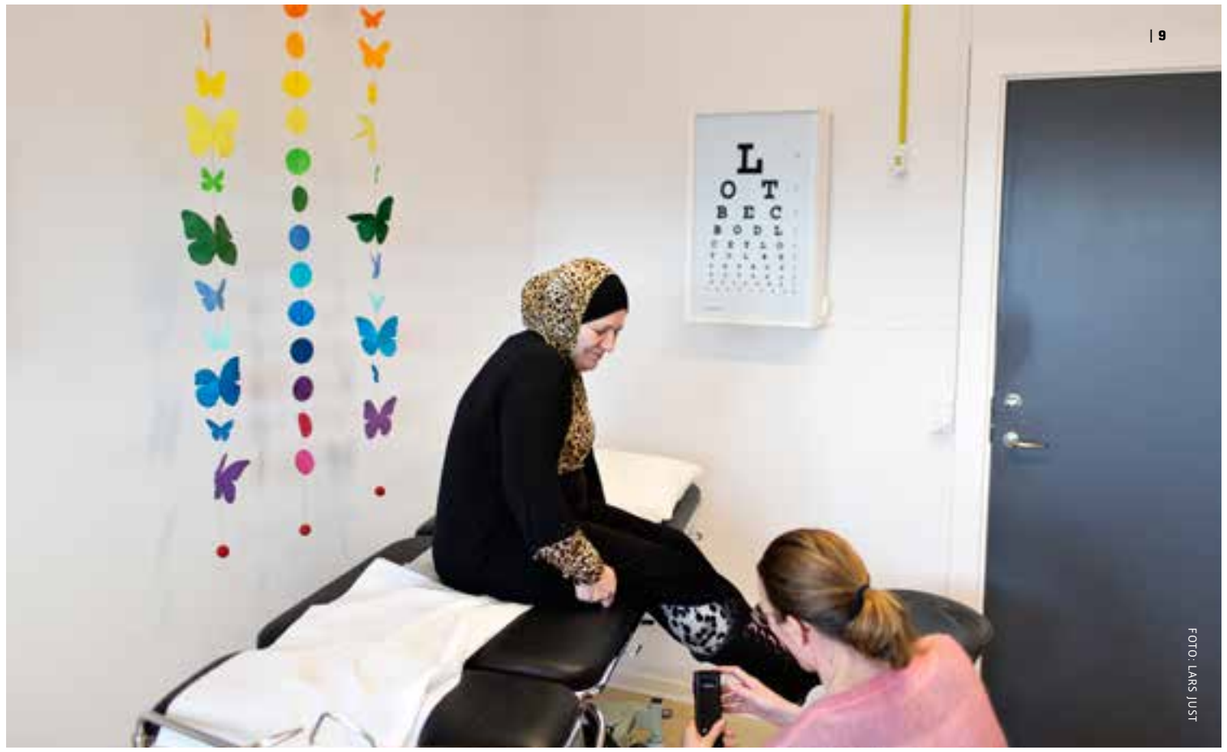
Din adgang til internettet er din udgang, men i høj grad også en adgang til at komme ind til dine oplysninger. Ethvert lokalt netværk er udsat for trusler mange gange i døgnet. Det er derfor vigtigt, at dit netværk er beskyttet af en firewall, som kun tillader kommunikation med parter, den kender (via VPN forbindelser), og at den er opdateret. Når du løbende opdaterer din firewall og opretholder en god praksis med kun at give adgang via VPN forbindelser med certifikat, har du sikret dit netværk på en af de bedste måder.

Derudover er det rigtig vigtigt, at du bruger adgangskoder og brugernavne, som har en vis kompleksitet, så adgangen ikke er let at gætte sig til.

Kravene til sikkerhed på nettet er i dag en smule lempeligere for private end for offentlige myndigheder. Men Datatilsynet kræver altid kryptering, når private

- overfører følsomme oplysninger via hjemmesider
- overfører personnumre via hjemmesider
- overfører oplysninger, der er underlagt særlige vilkår

Er du i tvivl, om du sender patientoplysninger på et åbent eller lukket netværk, bør du altid sende oplysningerne krypteret. Samtidig kan du med fordel sikre dig, at brugere kun har adgang til dit system ved hjælp af en tofaktorautentifikation, dvs. et system som brugeren kun kan anvende ved hjælp af to ting: noget som vedkommende *ved* og noget, som vedkommende *har*. Det mest kendte og udbredte eksempel på det er NemID. Der findes også andre muligheder på markedet, og du kan eksempelvis også anvende "sikker e-mail", hvor du med en digital signatur eller



NemID sikrer, at oplysninger i din mail er krypteret, og at mailen er signeret.

Dit lægesystem – en sikker løsning

E-mail og personfølsomme oplysninger går ikke i spænd. Der findes metoder til at sende sikre e-mails, men teknikkerne er mange, og det er sjældent, at disse understøttes af borgeren og/eller dine kollegaer. Det er derfor vigtigt, at du benytter de kommunikationskanaler, der er skabt til personfølsomme oplysninger. Her kan du til kollegaer benytte korrespondancemeddelelsen, som findes i dit lægesystem. Til borgeren bør du benytte de faciliteter, dit lægesystem stiller til rådighed i form af forskellige e-mail konsultationer.

Kommunikerer du via sundhedsdatanettet, er du på et sikret netværk. Det betyder, at der er indgået aftaler om, hvem der må kommunikere med hvem, så man ikke risikerer, at oplysningerne havner hos en forkert modtager. Men også på sundhedsdatanettet er der mulighed for, at oplysninger kan blive hacket af uvedkommende, og derfor anbefales det, at du altid krypterer følsomme oplysninger, inden du sender dem. Også på sundhedsdatanettet. Husk at stille krav om dette til din IT-leverandør.

Hvis du vil vide mere, kan du med fordel læse Datatilsynets "IT-sikkerhedstekst vedr. datatransmission af personoplysninger på åbne net".

Når du er i skyen

"Flere og flere brugere er begyndt at anvende Cloud-baserede løsninger, f.eks. Microsoft 365. Den slags løsninger skal overholde de samme krav til teknisk og organisatorisk beskyttelse af følsomme oplysninger, som hvis data befinder sig i et specifikt datacenter, f.eks. på serveren i din klinik eller hos din it-leverandør i Danmark. Hvis der er tale om en leverandør, som har datacentre uden for EU, skal du være opmærksom på, at der skal indgås en særlig EU-standardaftale for, at oplysningerne må lagres i Cloud-løsningen.

Anvender du produkter, som f.eks. Projectplace, Dropbox, One-drive eller lignende, skal du være opmærksom på, at disse løsninger kræver særlige tiltag for, at de må benyttes til at dele eller sende personoplysninger. Som standarder lever de nemlig ikke op til persondatalovens krav til databeskyttelse, fordi deres domicilland ligger uden for EU".

Husk

- Du kommer rigtigt langt med at bruge sund fornuft. Undlad at åbne mails med vedhæftede dokumenter eller links, som du har modtaget uopfordret
- Benyt kun de kommunikationsformer, dit lægesystem tilbyder til kommunikation med dine patienter og sundhedsvæsenets øvrige aktører
- Brug kun din PC i klinikken til arbejdsrelaterede opgaver
- Besøg kun hjemmesider, som du kender som troværdige, og undlad at surfe på må og få
- Adskil din private og din kliniks e-mailadresse, således at du adskiller dit privatliv fra dit arbejdsliv.
- Sæt klare retningslinjer for dine medarbejdere (du kan eventuelt benytte "Din arbejdsplads - dit ansvar" i appendiks A på side 15 i denne publikation)

Fysisk sikkerhed

Informationssikkerhed er ikke kun et spørgsmål om IT. Det handler også om oplysninger på papir, billeder, video m.v. Derfor spiller den fysiske sikkerhed – indretningen af din klinik – en vigtig rolle, så uvedkommende ikke kan få adgang til fortrolige oplysninger. Tænk derfor på, hvordan du indretter den del af klinikken, der er åben for patienter og pårørende. Vær f.eks. opmærksom på, hvor du placerer dine printere, skærme og storskærme og oversigtstavler, og sørg for, at klinikken som sådan er sikret mod indbrud og tyveri.

Ansvar og pligter

Du skal sikre, at der er én der har ansvaret for informationssikkerheden og sikre, at alle er bekendt med hvem, der har ansvaret.

Den ansvarlige skal sikre, at de retningslinjer, som den enkelte klinik har vedtaget, bliver efterlevet, og at god IT-skik er forankret godt i klinikken. Det medfører blandt andet et løbende tjek af:

- Det udstyr og de redskaber, der bruges ved behandling og opbevaring af informationer, og at de er sikret tilstrækkeligt mod tyveri, hærværk, brand, vandskade eller lignende
- Hvorvidt programmel (software-programmer) til beskyttelse mod malware/virus er opdateret
- Hvorvidt der dagligt sker back up af dine data, og at du får en kvittering for, at det er gået godt. En gang årligt bør du få læst din backup ind, så du sikrer dig, at backuppen også kan bruges til noget
- Dokumenterede nødprocedurer, hvis teknikken svigter og adgangene til klinikkens IT, EPM system, telefoni mv. ikke er funktionsdygtige. Dette dokument bør også indeholde kontaktoplysninger til alle relevante samarbejdsparter.
- At nødprocedurerne med mellemrum afprøves

Den fysiske sikkerhed er særlig vigtig, da fysisk adgang til din arbejdsplads og/eller server i mange tilfælde gør det nemt for en IT-kyndig at få fat i de data, der findes her.

Din server bør altid være udstyret med en UPS, der sikrer nødstrøm og nedlukning af serveren i tilfælde af strømafbrydelse. Når strømmen går, lukkes din server ikke korrekt ned, hvilket kan medføre, at data beskadiges eller går tabt. En UPS nødstrøm placeres mellem server og strømforsyning, og i tilfælde af et strømsvigt slår UPS'en nødstrøm til og overtager strømforsyningen i et givent antal minutter og nedlukker derefter serveren korrekt.

Mobile enheder

Alle i samfundet anvender i stigende omfang mobile enheder, smartphones, tablets eller bærbare PC'er i deres arbejde. Det gælder også aktørerne i sundhedsvæsenet. De mobile enheder bliver mere og mere avancerede, og langt de fleste har netadgang. Det betyder, at de er sårbare over for virus, malware, hvis de ikke er sikret tilstrækkeligt. Samtidig optræder små computere i snart sagt alt – det kan være ure, sko, kameraer, stikdåser m.v. Vi taler om Internet of Things.

Telemedicinske løsninger, hvor man anvender mobile enheder til at opsamle informationer fra patienter eller kommunikere med dem, bliver udbredt i stigende grad, og brugen af forskellige apps og enheder gør det svært at opretholde et forsvarligt sikkerhedsniveau.

I juridisk forstand skal apps, som anvendes med det formål at behandle sundhedsdata i behandlingssituationer, betragtes som medicinsk udstyr på linje med "stand-alone-software". Apps skal med andre ord også leve op til bl.a. persondatalovens krav. Eftersom mange apps er udviklet til privat brug, har udvikleren ikke nødvendigvis haft fokus på sikkerhed i forhold til trusler fra internettet. Du skal derfor altid kontrollere, om de apps, du bruger i telemedicinske løsninger, lever op til sikkerhedskravene. Læs eventuelt også Lægemiddelstyrelsens "CE-mærkningsordning".

Hvis det er patientens eget udstyr, der anvendes til at opsamle helbredsoplysninger, f.eks. i forbindelse med telemedicin, har du i sagens natur ikke direkte indflydelse på sikkerhedsniveauet i patientens mobile enhed. I de tilfælde skal du sørge for, at det program eller den app, som du anvender til at behandle oplysningerne, er tilstrækkeligt sikret.

Hvis de mobile enheder, du anvender, er tilknyttet et såkaldt MDM-system (Mobile Device Management) kan man f.eks. sikre sig, at der er adgangskontrol på de mobile enheder, at data opbevares krypteret, og at oplysninger på enheden kan slettes, hvis den bliver stjålet eller hacket.

Sådan kan du imødegå tyveri

Hvis nogen har fysisk adgang til din enhed, er din fortrolighed truet. Så det bedste råd, der kan gives er, at undgå at lagre data på bærbare enheder. Desuden bør bærbare PC'ere aldrig opbevares i bil eller andet sted, hvor de ikke er låst inde eller overvåget.

Husk også at

- sikre din tablet mod tyveri i samme omfang som din stationære arbejdsstation
- du ikke bør efterlade din PC, mobiltelefon eller laptop i bilen. Hav dem altid under opsyn eller låst inde
- der gælder samme regler om adgangskode på dine mobile enheder som på din faste installation. Bærbare harddiske og laptops bør være krypteret med Bitlocker[1] eller tilsvarende
- udføre back up på data fra dine mobile enheder. Data på bærbare computere kræver lige så megen sikkerhedskopiering/backup, som din faste installation. Måske i virkeligheden endnu mere, da de er mere udsatte end den faste installation
- sikre dine mobile enheder mod virus fra f.eks. apps, SMS/MMS og sociale medier. Bærbare computere er lige så udsatte for virus og anden malware. Derfor skal de altid have opdateret antivirus. Det skal særligt bemærkes, at en bærbar computer, der indeholder data, som kan henføres til patienter eller anden fortrolig information, aldrig bør benyttes som "familie-PC"
- beskytte din tablet mod snifferprogrammer, der kan opsnappe din kommunikation, når du anvender Wi-Fi i lufthavne, tog og lignende
- betragte eksterne netværk som fremmede. Ethvert offentligt netværk er en trussel mod sikkerheden. Vær opmærksom på dette – og hvis du benytter opkoblinger til din klinik, så er det ikke nok med fjernstyringssoftware, men det anbefales, at du får en VPN forbindelse sikret med certifikat.

[1] **Bitlocker** er en krypteringsmekanisme, der blev introduceret til Windows Vista, og som benyttes til at kryptere data på lagringsmedier.

Afslutning

Som nævnt er de praktiserende læger en vigtig del af det sammenhængende danske sundhedssystem. Derfor er det også vigtigt, at der er en stærk bevidsthed om informationssikkerheden i almen praksis. En sikker omgang med og adgang til informationer er en forudsætning for en høj kvalitet i din patientbehandling samt en sikker drift af din klinik, og det har i høj grad betydning for almen praksis' omdømme i samfundet.

Håbet er, at denne publikation har bidraget til at styrke og kvalificere dit arbejde med informationssikkerhed. Publikationen kan på ingen måde dække alle sundhedssektorens aspekter og regler inden for informationssikkerhed, men savner du svar på et eller flere basale spørgsmål, eller har du gode idéer til videreudvikling af publikationen, er du meget velkommen til at maile til mib.plo@dadl.dk.

FOTO: LARS JUST

Litteraturliste

Nedenstående liste er primært en oversigt over love, bekendtgørelser og vejledninger. Listen er på ingen måde fyldestgørende og indeholder kun de kilder, der vurderes at have størst relevans for almen praksis.

- Arkivloven (Bekendtgørelse af arkivloven). Lovbekendtgørelse nr. 1035 af 21. august 2007
- Bekendtgørelse om indberetning af oplysninger til kliniske kvalitetsdatabaser m.v., bekendtgørelse nr. 1725 af 21. december 2006
- Forsikringsaftaleloven, lovbekendtgørelse nr. 1237 af 9. november 2015
- Journalføringsbekendtgørelsen (journalføring, opbevaring, videregivelse og overdragelse), bekendtgørelse nr. 3 af 2. januar 2013
- Offentlighedsloven, (Lov om offentlighed i forvaltningen), lov nr. 606 af 12. juni 2013
- Persondataloven (Lov om behandling af personoplysninger) lov nr. 429 af 31. maj 2000
- Principper om de praktiserende lægers deling af journaloplysninger (PLO) http://www.laeger.dk/portal/pls/portal/!PORTAL.wwpob_page.show?_docname=11027470.PDF
- Sikkerhedsbekendtgørelsen (Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning), bekendtgørelse nr. 528 af 15. juni 2000
- Sundhedsloven (Bekendtgørelse af sundhedsloven), lovbekendtgørelse nr. 1202 af 24. november 2014
- Vejledning om informationssikkerhed i sundhedsvæsenet, Sundhedsdatastyrelsen april 2016
- Vejledning til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, vejledning nr. 327 af 2. april 2001
- Datatilsynet, Behandling af personoplysninger i cloudløsningen Office 365, brevdato: 06.06.12, journalnummer: 2011-082-0216
- Datatilsynet (2014). It-sikkerhedstekst ST1. Flere faktorer i login
- Datatilsynet (2014). It-sikkerhedstekst ST2. Overvejelser om sikring mod, at personoplysninger kommer til uvedkommendes kendskab i forbindelse med datatransmission
- Datatilsynet (2014). It-sikkerhedstekst ST4. Datatransmission af personoplysninger på det åbne net
- Digitaliseringsstyrelsen (2015). Informationssikkerhedspolitik
- Digitaliseringsstyrelsen (2015). Sikker e-mail – Om Nem-ID
- EU-persondataforordningen, implementeres i dansk lov med virkning fra 25. maj 2018
- MedCom (2015). Infrastruktur. Det danske sundhedsdatanet

Appendiks A.

Forslag til:
Din arbejdsplads – dit ansvar

Fysisk arbejdsplads og PC
Brugen af bærbare PC'er, tablets, mobil og lign. håndteres efter samme retningslinjer, som arbejdspladsens faste installationer.

De af klinikken udleverede PC/tablet må kun anvendes til arbejdsmæssige formål

Din PC, usb og eksterne harddisk må kun indeholde programmer, som klinikken har godkendt, samt arbejdsrelaterede filer. Vær særlig opmærksom på download af filer (kun arbejdsrelateret) fra internetsider, som du ikke har tillid til. Din PC må aldrig tilsluttes eksterne enheder, som du ikke kender eller har tillid til.

Arbejdet i klinikken indebærer adgang til personfølsomme data. Medarbejderen skal derfor være særlig opmærksom på, at:

- PC'en er opdateret med seneste version af antivirus
- de benyttede programmer er opdateret
- undlade at notere password på papir og lignende
- undgå at kollegaer ser med, når du taster dine passwords
- personlige passwords ikke må udlånes/oplyses til andre
- logge af på din PC eller din mobile enhed, når du forlader den
- du ikke må udveksle personfølsomme data (ukrypteret) via e-mail, messenger, chat m.m.

Ved arbejdstids ophør skal PC'en slukkes og mobile enheder logges af. Alle arbejdspapirer skal placeres på en struktureret måde i bakker, mapper, skuffer m.m., således at papir ikke ligger fremme, og bordet er ryddet, når man går hjem.

I forbindelse med håndtering af fortrolige dokumenter og lign. er det vigtigt at huske at lægge materialet til makulering. Alle udskrifter, breve mv., der indeholder personfølsomme data, skal makuleres.

Bærbare enheder
Bærbare enheder omfatter laptop, tablet, kindle, mobiltelefon, projekter, ekstern harddisk, USB mv.

Ved brug af bærbare enheder, dokumenter samt dialog i mobiltelefon uden for klinikken og i offentligt rum generelt, skal der altid udvises høj diskretion. Vær altid meget opmærksom på, at uvedkommende kan kigge over skulderen og aflure passwords og dermed få adgang til indhold i mailkorrespondance, personfølsomme data etc.

I undervisningssituationer skal der altid foretages log-in inden skærmbillede vises synligt på projektor og storskærm.

Det er altid medarbejderens pligt, at dokumenter og enheder opbevares forsvarligt både under transport samt under/efter brug. Opbevar altid dokumenter/enheder ikke-synligt i aflåst rum/hus, når de ikke benyttes.

Hvis du er nødt til at opbevare dokumenter eller enheder i køretøj, må de ikke være synligt tilgængelig, når køretøjet forlades.

USB, ekstern harddiske og andre lageringsmedier
Eksterne lageringsmedier skal altid være krypteret, såfremt de forlader arbejdspladsen.

FOTO: LARS JUST

PRAKTISERENDE LÆGERS ORGANISATION

Kristianiagade 12
2100 København Ø