INFORMATIONSSIKKERHED:

Hvad kan jeg selv gøre i min praksis?

I takt med øget digitalisering og datadeling stiger risikoen for hackerangreb og it-kriminalitet. Interessen for informationssikkerhed i sundhedsvæsenet er stigende, og der er øget efterspørgsel fra såvel både borgere og myndigheder. Her kan det være svært at danne sig et overblik over hvad, man som speciallæge skal være særligt opmærksom på. Sundheds- og Ældreministeriet har i samarbejde med Deloitte derfor udarbejdet disse kliniknære anbefalinger, som kan guide speciallægen til at højne informationssikkerheden i klinikken.

1. Sørg for klare aftaler om ansvar og arbejdsdeling med systemleverandøren

- Gennemgå leverandørkontraktens afsnit om sikkerhed og stil spørgsmål til leverandøren, hvis du er i tvivl om noget.
- Spørg ind til konkrete situationer (hackerangreb, mistanke om fortrolighedsbrud mv.). Hvem har ansvaret? Hvem tager initiativ?
- Bed systemleverandøren afklare, om automatisk systemopdatering er slået til på dine computere og for journalsystemet – samt hvordan du selv kan se, om de nyeste opdateringer er implementeret.
- Indhent bekræftelse fra leverandøren på, at den version af journalsystemet som I anvender, krypterer patientdata.

2. Indgå en serviceaftale for informationssikkerhed

- Etablér en serviceaftale med en it-serviceleverandør, så du kan ringe efter hjælp i tilfælde af angreb eller nedbrud – det er vigtigt på forhånd at vide hvor, man kan ringe efter hjælp.

3. Opsæt informationsmateriale og træn awareness

- Brug visuelle virkemidler til at sikre, at informationssikkerhed bliver en naturlig del af hverdagen. Virkemidler kan findes på *sikkerdigital.dk/virksomhed/fem-gode-raad-der-styrker-din-virksomheds-it-sikkerhed/faa-gode-digitale-vaner*
- Planlæg årlig træning i informationssikkerhed – kan både være fysiske øvelser med en ekstern ekspert eller online awareness-kurser. Spørg evt. din leverandør om de tilbyder dette.
- Tænk god it-hygiejne og god brugeradfærd ind i jeres intro-forløb for nye medarbejdere. Introducer her medarbejderne til de vejledning, som der linkes til nedenfor.

4. Fastsæt interne retningslinjer for klinikkens it-sikkerheds-hygiejne

- Alle nye ansatte, også uddannelseslæger, skal introduceres til it-sikkerhedsrutiner.
- Personale skal lukke programmer ned og efterlade en låst skærm, når de forlader arbejdsstationen.
- Der skal anvendes privacyfiltre på skærmene de steder, hvor uvedkommende (patienterne/andet klinikpersonale) har mulighed for at se skærmen.
- Brugeradgang/password må ikke deles eller skrives ned.
- Sæt lås på relevante skuffer og arkivskabe for at beskytte informationer.
- Sørg altid for at konsultationen forbliver privat – fx ved at lukke døre eller på anden vis skærme.
- Brug af private smartphones bør begrænset i videst muligt omfang, og disse bør ikke ligge fremme.
- Private enheder må ikke tilkobles netværket.
- Private ærinder på arbejdscomputere bør i videst muligt omfang begrænses og bør kun ske med en separat brugerprofil med begrænsede rettigheder. Private mailkonti og sociale medier må således kun tilgås med en separat brugerprofil – eller slet ikke.
- Ankomststanderen må ikke vise patienternes CPR.
- Eventuelle servere skal være låst inde.
- Unødvendige åbne usb-porte skal være deaktiveret/tildækket.
- Administratorrettigheder skal begrænses til det strengt nødvendige.
- Slet eller deaktivér brugere ved off-boarding af personale, herunder login til Windows samt lægesystem, sundhed.dk, medarbejdersignatur via nemid.dk, FMKonline (medhjælps-adgange) og virk.dk.
- Slet CV, ansøgning og andet persondata på tidligere ansatte.
- Alle programmer skal opdateres jævnligt.
- Password skal skiftes ved fastsatte intervaller. Kompleksitet og længde skal tilsikres og historik slås til.
- Håndtering af informationssikkerheden i klinikken skal årligt kontrolleres af en ekstern rådgiver.

5. Tag stilling til håndtering af nød-situationer og til brugernes adgange

- Planlæg hvad klinikken skal gøre, hvis systemerne er utilgængelige. Vigtigst hvordan arbejdet kan fortsætte, men også hvem der skal orienteres, hvor de relevante telefonnumre er osv.
- Hvilke processer kan fortsætte offline (udarbejd eventuelt skabeloner, der kan understøtte arbejdsgangene), og hvordan tilsikres det, at den manuelle behandling af følsom information er tilstrækkeligt sikker?
- Kontakt systemleverandøren for at minimere brugeradgange til det nødvendige.
- Aftal internt en klar proces for brugeradministration og løbene kontrol af relevante brugeradgange (eksempelvis at en medarbejder i klinikken kvartalsvis skal gennemgå alle adgange).

6. Tjek klinikkens backupaftale

- Tages der kun backup af lægesystemet? Eller også af fællesdrev?
- Hvor ofte tages der backup, og tester leverandøren, om det virker? Vurdér om det er tilstrækkeligt.

7. Begræns opkobling af udstyr på internettet

- Begræns opkobling af udstyr på internettet (eksempelvis printere) og påse tilstrækkelig fysisk sikring af udstyr (eksempelvis ved brug af kabellåse eller aflåste skabe).

8. Få foretaget en årlig sårbarhedstest af klinikkens it-miljø

- Få foretaget en årlig sårbarhedstest af jeres it-miljø. Tænk eventuelt dette sammen med jeres awarenesstræning.
- Dem som hjælper klinikken med at foretage en sårbarhedstest skal bl.a. dække følgende:
  - *Kontrollér at proces for brugeradministration overholdes, og at klinikken foretager brugerreview/oprydning.*
  - *Kontrollér opdatering af systemer, firewall, antivirus samt om harddiske er krypterede og porte blokerede.*
  - *Kontroller wi-fi-indstillinger og anvendelse af netværkskryptering. Der kan med fordel foretages enhedsfiltrering (MAC) på netværket – så kun godkendte enheder kan tilgå netværket.*
  - *Vurdér nødvendigheden af et gæstenetværk, hvis dette anvendes.*

9. Undersøg muligheder for sikker kommunikation med patienter

- Undersøg om din systemleverandør kan hjælpe med sikker mail.
- Få hjælp til implementering af en teknisk forsvarlig løsning til kommunikation med patienter (eksempelvis en portal hvor historik gemmes og hvor kommunikationen er krypteret).

NYTTIGE LINKS

Vejledning omkring informationssikkerhed i leverandørforhold (www.sikkerdigital.dk)
Vejledning omkring hændelseshåndtering (www.sikkerdigital.dk)
Vejledning vedr. brud på persondatasikkerheden (www.datatilsynet.dk)
Indberet sikkerhedshændelser vedr. persondata (www. virk.dk)

SUNDHEDS- OG ÆLDREMINISTERIET

Deloitte.