Deloitte.
Digital

Juni 2020

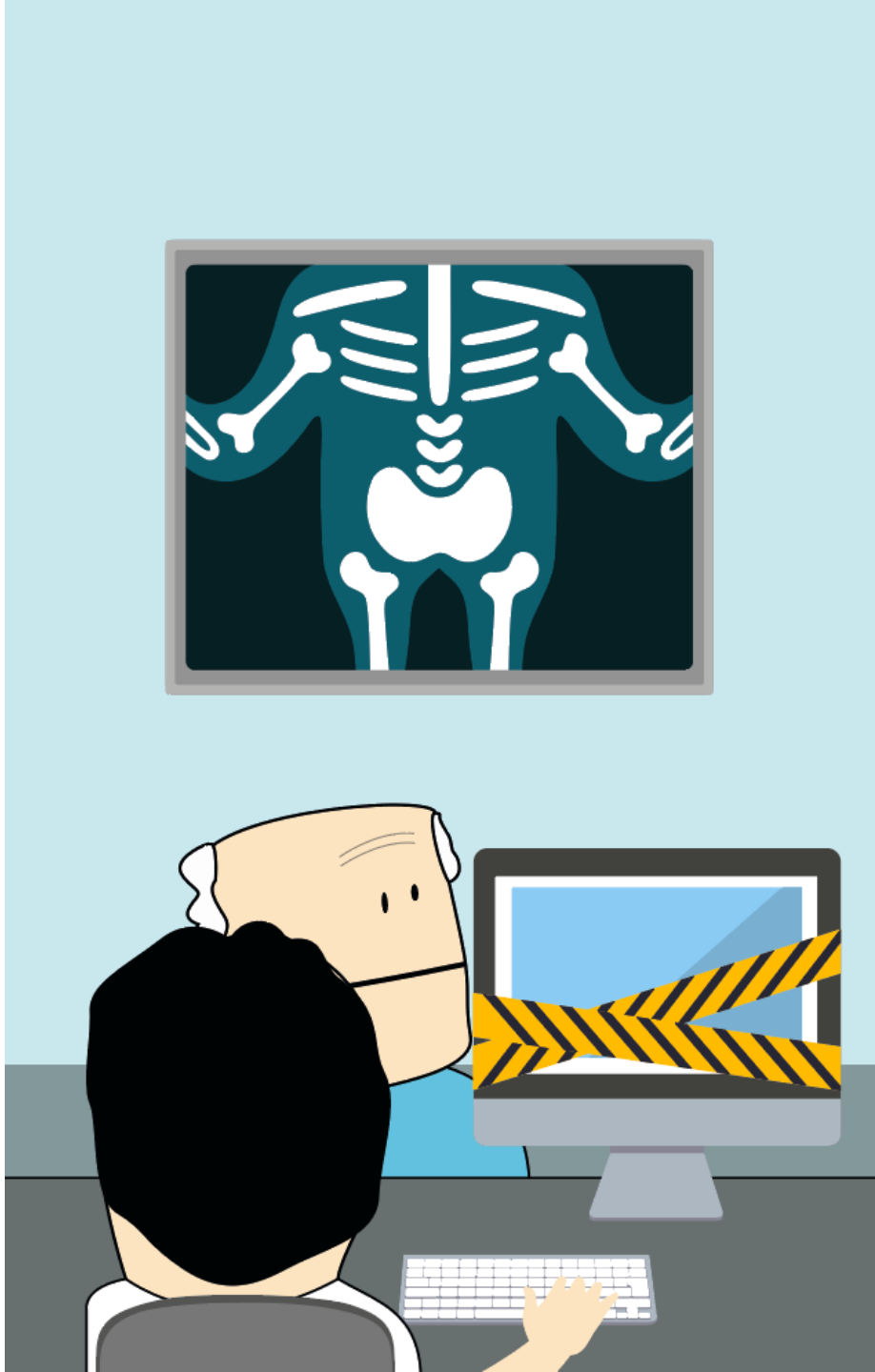
# Analyse af cyber- og informationssikkerhed

blandt praktiserende speciallæger

SUNDHEDS- OG ÆLDREMINISTERIET

FAS

DANSKE REGIONER



# Det har vi hørt...

*"Vi kan altid ringe til vores systemleverandørs hotline eller direkte til deres teknikere i særlige tilfælde."*
*Praktiserende speciallæge*

*"Gid jeg havde en der kunne rådgive mig. En der snakker dansk og ikke 'it', og som i hyppige intervaller gennemtjekker det hele."*
*Praktiserende speciallæge*

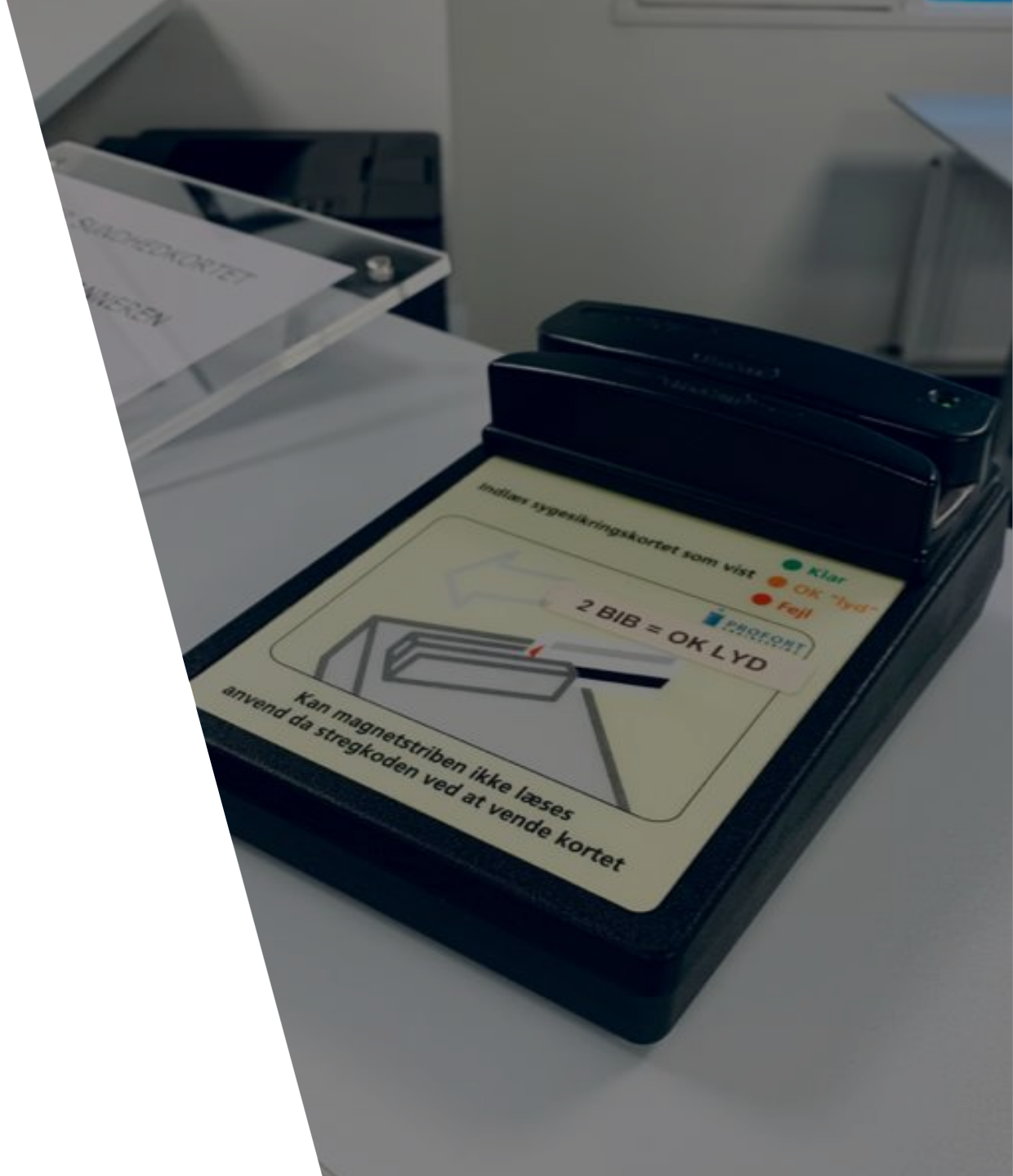
*"Jeg er en dygtig læge. Jeg er ikke uddannet i it. Jeg forstår ikke det sprog; derfor betaler jeg mig fra det, og så må jeg håbe, at min leverandør har styr på det."*
*Praktiserende speciallæge*

*"Man overleverer glædeligt ansvaret [til systemleverandøren], for man betaler jo for det, men nu hvor du stiller det spørgsmål, tænker jeg, at jeg burde have været mere kritisk."*
*Praktiserende speciallæge*

# Indholdsfortegnelse





# Konklusion

Fra speciallægen åbner sin klinik om morgenen til klinikken aflåses og lukkes om aftenen er der i alle sekvenser identificeret potentielt sårbare situationer. De praksisnære observationer falder i syv kategorier:

1) *Manglende kendskab til konsekvenser ved utilstrækkelig sikkerhed*
2) *Uklarhed om eget ansvar og krav til systemleverandør*
3) *Adgangsrettigheder og identiteter deles på tværs af personale*
4) *Manglende procedurer som fx beredskabsplaner og on- og off-boarding*
5) *Manglende sikkerhedshærdning af it-udstyr*
6) *Utilstrækkelig adgangs-styring*
7) *Ikke-sikker korrespondance (bl.a. mail).*

Der er konstateret stor spredning i klinikkernes informationssikkerhedsniveau, og klinikker med adgang en informationssikkerhedsfaglig rådgiver har en højere sikkerhed. Der er endvidere generelt mere fokus på den juridiske del (GDPR mv.) end den mere tekniske ende af informationssikkerheden. De klinikker, der er mest opmærksomme på informationssikkerheden, savner stadig praktiske værktøjer og har endvidere generelt en forventning om, at leverandøren har et mere udstrakt ansvar end tilfældet er.

Analysen opstiller tre sæt af anbefalinger: kliniknære, leverandørvendte og tværgående (se s. 20ff). Det anbefales endvidere, at der på et tværgående niveau så vidt muligt også igangsættes initiativer, som understøtter lægerne i deres arbejde med de kliniknære anbefalinger.

For den enkelte praktiserende speciallæge uden egen it-organisation er det afgørende, at man på overskuelig vis kan navigere i informationssikkerheds-kravene og på baggrund heraf effektivt kan gennemføre foranstaltninger, som sikrer et passende beskyttelsesniveau. Dette vanskeliggøres af fraværet af målrettede, praksisnære vejledninger og værktøjer. Det vanskeliggøres også af den gensidige usikkerhed om minimumskrav læger og leverandører imellem. Endelig vanskeliggøres det af, at informationssikkerhed i mindre grad er værktøjsmæssigt og organisatorisk forankret i sektoren.

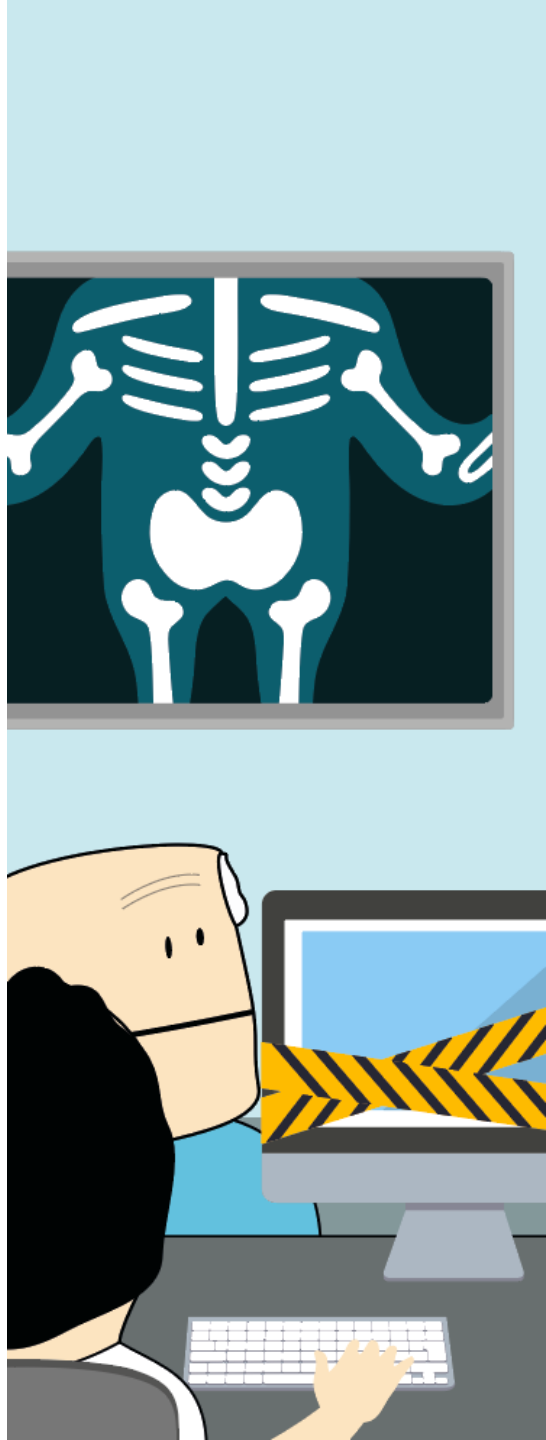
Til sammenligning er der inden for patientsikkerhedsområdet målrettede værktøjer og en kendt understøttende organisering – samt en erkendelse af (awareness om), at patientens *sikkerhed* er en del af lægens forpligtelse. Hvad angår patientens *datasikkerhed* vurderes der at være behov for tilsvarende – såvel værktøjer som organisation og awareness. På organisationssiden er det bl.a. anbefalet, at der besluttes en skalerbar model for en ordning i stil med den, som de regionale datakonsulenter nogle steder varetager.

For borgerne handler det om, at man kan blive ved med at have tillid til lægens omgang med sine persondata, herunder at data ikke forvanskes eller på anden vis kompromitteres. For staten og regionerne handler det ydermere om, at der i alle led af sundhedsvæsenets værdikæde opretholdes et passende informationssikkerhedsniveau. Analysen har vist, at nogle læger selv gør en stor indsats for informationssikkerheden, samt at nogle leverandører tilsvarende læner sig over mod deres kunder med anbefalinger om at høje sikkerheden. Men i et nationalt perspektiv er det for skrøbeligt at forlade sig på ildsjæle. Uanset sektoransvarsprincippet må det være en fælles ambition for parterne – herunder særligt SUM, SDS (DCIS), FAPS, PLO og Danske Regioner – at tilvejebringe et mere robust grundlag for primærsektoren.

Den enkelte læge kan gøre meget for højne sikkerheden af omgang med personfølsomme data i klinikken, men det kan ikke rimeligvis forventes, at den enkelte læge eksempelvis skal vurdere de 100+ ISO-kontroller og herudfra bl.a. definere minimumskrav til leverandøren, endsige føre tilsyn hermed (hhv. afkode de modtagne tilsynsrapporter). Det kan heller ikke rimeligvis forventes, at den enkelte læge selv følger med i trusselsbilledet og løbende tilpasser sine foranstaltninger til en kombination af trusselsbilledet og risikoappetitten. Her argumenteres der i stedet for, at man kan komme langt med at blive enige om anbefalede minimumskrav og et sæt af basiskontroller, som man mere "mekanisk" og tjeklistebaseret kan holde sig op imod.

***"Jeg er en dygtig læge. Jeg er ikke uddannet i it. Jeg forstår ikke det sprog, derfor betaler jeg mig fra det også må jeg håbe at min leverandør har styr på det." –*** *Praktiserende speciallæge*

På it-siden bør der foruden de basale kontroller og foranstaltninger også mere grundlæggende tages hensyn lægens forhold og arbejdssituation allerede ved design og videreudvikling af systemer og andre services, således at der designes løsninger, der med informationssikkerheden som et integreret element understøtter en travl hverdag, i stedet for at modarbejde den. Speciallægen bør ses som det potentielt stærkeste led og bør hjælpes til at indtage denne position, så der både i den enkelte klinik og i det samlede væsen fortsat kan være høj tillid til omgangen med patienterne og deres data.



# Opsummering af anbefalinger

Analysen har udviklet anbefalinger inden for tre kategorier. De er i kortform opsummeret nedenfor og udfoldes nærmere i ledelsesresumeet.

## SPECIALLÆGEKLINIKKEN

**Kliniknære anbefalinger**

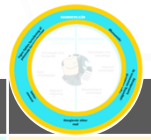
**Behov for tættere samarbejde**

1. Sørg for klare aftaler om ansvar og arbejdsdeling med systemleverandøren
2. Etablér en serviceaftale for informationssikkerhed
3. Opsæt informationsmateriale og træn awareness
4. Udarbejd en intern beskrivelse af klinikkens it-hygiejne
5. Tag stilling til håndtering af nødsituationer og til brugeres adgange
6. Tjek klinikkens backupaftale
7. Begræns opkobling af udstyr på internettet
8. Få foretaget en årlig sårbarhedstest af klinikkens it-miljø
9. Sørg for sikker kommunikation med patienter

## SYSTEMLEVERANDØREN

**Leverandørvendte anbefalinger**

1. Gennemgå kontrakten sammen med speciallægen
2. Indtag en sparrende rolle over for speciallægen
3. Tilsikr at data er krypteret i journalsystemet
4. Tilsikr at forbindelsen til SDN-knudepunktet er krypteret
5. Tilbyd sårbarhedsscanninger
6. Indgå dialog med speciallægen omkring en teknisk forsvarlig løsning til kommunikation med patienter
7. Anse styrkelse af interne processer for it-sikkerhed som et konkurrenceparameter



## TVÆRGÅENDE FORHOLD

**Nationale anbefalinger (rådgivning, tilsyn, sikker mail mv.)**

**Definer minimumskrav**

1. Udbyg og målret sikkerdigital.dk.
2. Understøt klinikkerne med informationstiltag
3. Etabler en entydig indgang til rådgivning
4. Udstik anbefalede minimumsstandarder for sektoren
5. Udbred sikker mail
6. Aftal hændelseshåndtering med systemleverandørerne
7. Analyse af forbundet medicoapparatur
8. Kræv kryptering på Sundhedsdatanettet og afklar ansvar for databehandleraftaler på tværs


# 1. Ledelses-resume og anbefalinger

# Indledning

Sundhedsvæsenet er genstand for et stigende og stadig mere komplekst risikobillede, hvilket stiller større krav til såvel procesmæssige som tekniske foranstaltninger. Efter en årrække med GDPR og tiltag omkring de primært juridiske aspekter ved omgangen med patientdata begynder der nu at være et mere systematisk fokus på de tekniske og adfærdsmæssige foranstaltninger, som i praksis er helt afgørende for en sikker og tillidsvækkende omgang med patientdata. Dette fokus er understøttet af sundhedssektorens cyber- og informationssikkerhedsstrategi fra januar 2019. Nærværende analyse har således også sit fokus på de praktiske foranstaltninger, der kan bidrage til et højere niveau af informationssikkerhed såvel i den enkelte klinik som på tværs af forsyningskæden.

Det er ikke længere et spørgsmål om hvorvidt, virksomheder rammes af cyberangreb – men hvornår og hvordan, man tackler et angreb. Det er et stressende forløb, hvor der opstår en masse spørgsmål. Her er det vigtigt med en køreplan: Hvor skal man ringe hen, hvordan kommer vi tilbage på sporet, hvad siger vi til vores kunder, og skal vi indrapportere brud på persondatasikkerheden?

Et trygt, sikkert og sammenhængende sundhedsvæsen kræver en sikker primærsektor, herunder speciallægepraksis. De enkelte speciallægeklinikker er typisk små virksomheder, og den enkelte kan med en række konkrete indsatser gøre mere i det daglige. Betingelserne for at forbedre sikkerheden ligger dog i høj grad også i samspillet mellem læge og leverandør. Analysen viser, at dette samspil fortsat fremstår uklart – således er den generelle opfattelse, at leverandøren har et mere udstrakt ansvar for den tekniske sikkerhed, end tilfældet egentlig er. Den enkelte klinik har endvidere ikke nok at støtte sig til i en dialog med sin leverandør om hvad, der er passende foranstaltninger. En væsentlig forudsætning for at løfte sektoren vil således være, at der fra et tværgående niveau i højere grad støttes op omkring de enkelte lægers ansvar. Nærværende analyse har fokus på det kliniknære, men favner dog begge perspektiver: Både individuelle forbedringstiltag til den enkelte klinik og mere tværgående tiltag, der tilsiger, at enten myndigheder eller leverandører af patientjournalsystemer læner sig mere ind mod de små lægevirksomheder og understøtter arbejdet med informations-sikkerhed – og dermed bidrager til, at lægen som dataansvarlig effektivt kan efterleve sit ansvar. Anbefalingerne vurderes samlet set at kunne fastholde en høj tillid til lægerne.*

*) En analyse fra 2019 viser, at patienterne har høj tillid til praksissektorens omgang med patientdata: Blandt respondenter, som ikke vil dele helbredsdata med deres læge, svarer kun 4%, at dette skyldes informations-sikkerhedsmæssige bekymringer (Deloitte 2019 Global Health Care Consumer Survey).

## Analysen i hovedtal

**06**
Klinikbesøg

**06**
Leverandørinterviews

**92 %**
af speciallægernes systemleverandører er inkluderet**

**21**
Patientkonsultationer

**09**
Personaleinterviews

**5 ud af de 15**
specialer er omfattet

Analysen omfatter også interviews med:

**DCIS, PLO, MedCom og regional datakonsulent**

## Konkrete anbefalinger til at højne informationssikkerheden

**09**
Kliniknære anbefalinger

**07**
Leverandørvendte anbefalinger

**08**
Tværgående anbefalinger

**) Opgjort efter markedsandele. 75 % er både interviewet og afdækket gennem klinikbesøg.

# Hvorfor er informationssikkerhed vigtigt?

Et brud på persondatasikkerheden kan for eksempel rent teknisk ske, når den dataansvarliges it-systemer ikke er tilstrækkeligt sikrede, så udefrakommende får adgang til oplysningerne (for eksempel via hacking). Det kan imidlertid også være den dataansvarliges egen håndtering af personoplysningerne, der kan forårsage et brud. Det gælder for eksempel, hvis den dataansvarlige ubeføjet videregiver eller ændrer personoplysninger. Datasikkerhed handler ikke kun om fortrolighed, men også at om, at datas integritet (korrekthed) og datas tilgængelighed sikres. Nedenstående illustrerer forskellige bekymringsscenarier.

## Vi er alle enige om, at dette ikke må ske

Tænk hvis jeg ikke kunne stole på, at data i systemet er korrekt?

Tænk hvis systemet ikke var tilgængeligt, når jeg skulle bruge det?

Tænk hvis mine patienters oplysninger blev lækket?


Praktiserende speciallæge

Tænk hvis jeg ikke kunne stole på, at medicinen i FMK var rigtig?

Tænk hvis jeg ikke kunne være sikker på, at mine oplysninger bliver behandlet med fortrolighed?

Tænk hvis data i mine patienters journaler blev ændret eller byttet rundt?

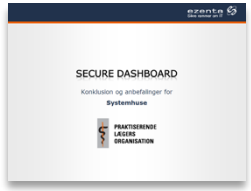

Patient

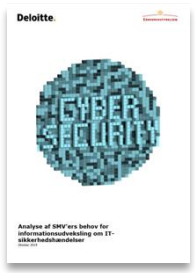
# Analysen bygger ovenpå eksisterende bidrag

Analysen bygger oven på eksisterende bidrag, særligt en analyse af praksissektorens systemhuse, hvis konklusioner også vurderes at gælde for speciallægerne. Samarbejdet mellem leverandør og klinik har generelt vist sig afgørende for niveauet af informationssikkerhed hvilket skærpes af fraværet af alternative kilder til rådgivning og vejledning.


**Sundhedssektorens cyber- og informationssikkerhedsstrategi 2019-2022 (2019)**




**Analyse af praksissektorens systemhuse (2017 og med opfølgning i 2018)**




**Analyse af SMV'ers behov for informationsudveksling om IT-sikkerhedshændelser (2019)**

Den første samlede nationale strategi for cyber- og informationssikkerhed i sundhedssektoren, der samtidig markerede, at sundhed blev udpeget som én af seks samfundskritiske sektorer. Er aktuelt under udmøntning gennem en serie initiativer. I samme forbindelse er der i november 2018 oprettet en decentral cyber- og informationssikkerheds-enhed (DCIS) i Sundhedsdatastyrelsen, der skal fungere som knudepunkt og understøtte sektorens implementering af strategien. For almen praksis er 2017-analysen omtalt samt PLOs informationstiltag i forlængelse heraf. Praktiserende speciallæger er ikke særskilt omtalt, men foruden nærværende analyse er der i DCIS' regi også fokus på sektorens selvstændige erhvervsdrivende, herunder praksislæger og andre behandlere.

Analysen viste, at alle otte systemhuse præsenterer tilfredsstillende fysisk sikkerhed på deres systemer og har en ansvarlig omgang med informationer. Analysen viste dog også, at ingen af systemhusene havde påtaget sig det fulde sikkerhedsansvar for deres kunder, samt at lægerne som kunder i begrænset grad efterspørger ekstra sikkerhed. Det konkluderes således, at "*PLO's medlemmer har en forventning om, at ansvaret for deres IT-sikkerhed ligger hos det enkelte systemhus. Ezenta har ikke fundet grundlag for, at dette skulle være tilfældet.*" Tre af leverandørerne manglende endvidere dokumentation for deres processer og blev efterfølgende gentestet i 2018, hvor der fortsat var mangler, ligesom der i øvrigt blev konstateret en "ad-hoc tilgang til awareness".

Analysen havde fokus på hvilke særlige behov, SMV'er (små og mellemstore virksomheder) har inden for håndtering af informationssikkerhed, særligt angående informationsudveksling. Analysen viste generelt, at SMV'erne har vanskeligt ved selv at fastlægge et tilstrækkeligt beskyttelsesniveau, samt at de har svært ved at finde autoritative kilder til rådgivning, som er relevante og konkret handlingsanvisende. Analysen anbefaler bl.a. at sikkerdigital.dk gøres mere brugerorienteret samt at der etableres SMV-rettede sikkerhedstjek.

# Konteksten er samtidig en praksissektor i udvikling

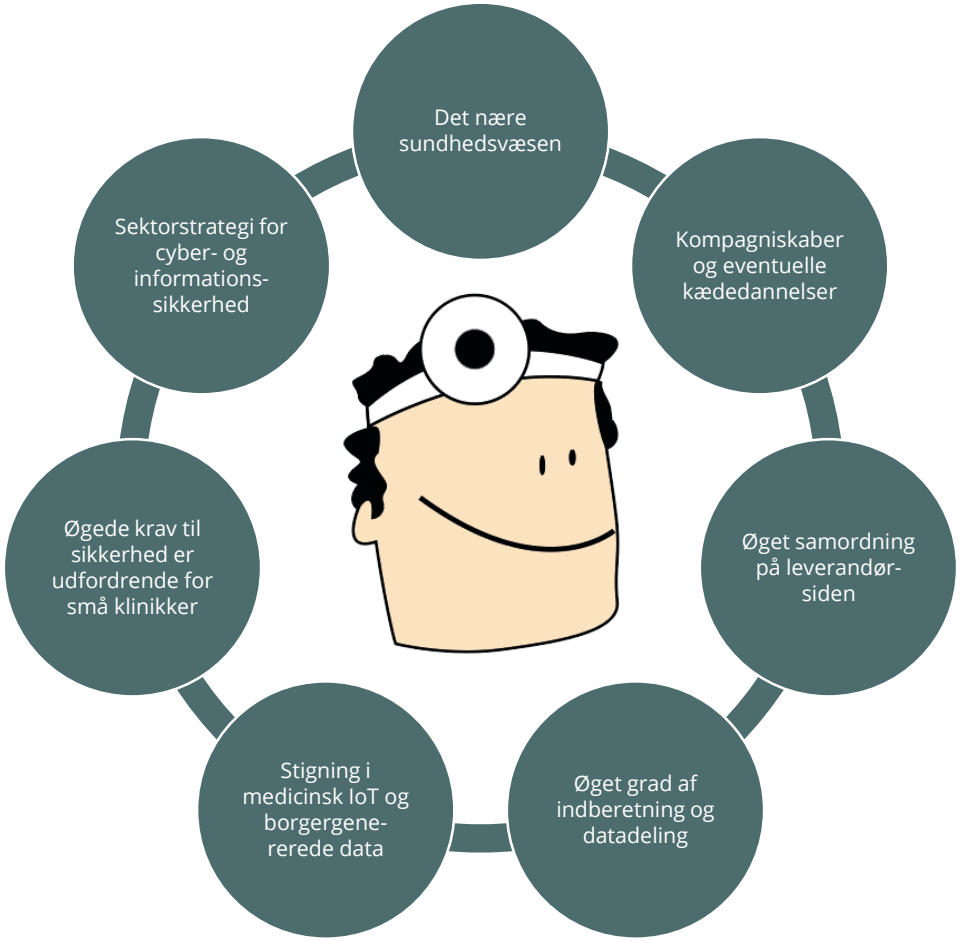
I takt med øget digitalisering og datadeling stiger risikoen for hackerangreb og it-kriminalitet. Interessen for informationssikkerhed i sundhedsvæsenet er stigende, og der er øget efterspørgsel fra såvel både borgere som myndigheder. Små erhvervsdrivende skal her navigere i nye typer krav.

Som en central del af det samlede sundhedsvæsen er praksissektoren genstand for øget bevågenhed i forhold til informationssikkerhed fra såvel myndigheder som borgere. Sektorstrategien for cyber- og informationssikkerhed driver på den ene side en efterspørgsel, men fører i takt med sin udmøntning samtidig til, at der trinvist etableres et bedre fælles fundament på tværs af sundhedsvæsnet – hvilket dog i mindre grad hjælper primærsektoren, der fortrinsvis består af små virksomheder uden egen it-organisation.

Parallelt hermed ses en bevægelse mod øget datadeling på tværs af sektorskel, for både primær (behandling) og sekundær anvendelse af data, hvilket skærper behovet for et tilstrækkeligt beskyttelsesniveau. Teknologisk giver stigningen i databærende forbundne devices og medicinsk IoT også anledning til nye typer risici.

I primærsektoren ses en vis bevægelse mod øget samordning. Særligt har leverandørerne organiseret sig i et fælles forum. I kombination med sektorstrategien er der således skabt et bedre grundlag for at adressere informationssikkerhedsmæssige problemstillinger.

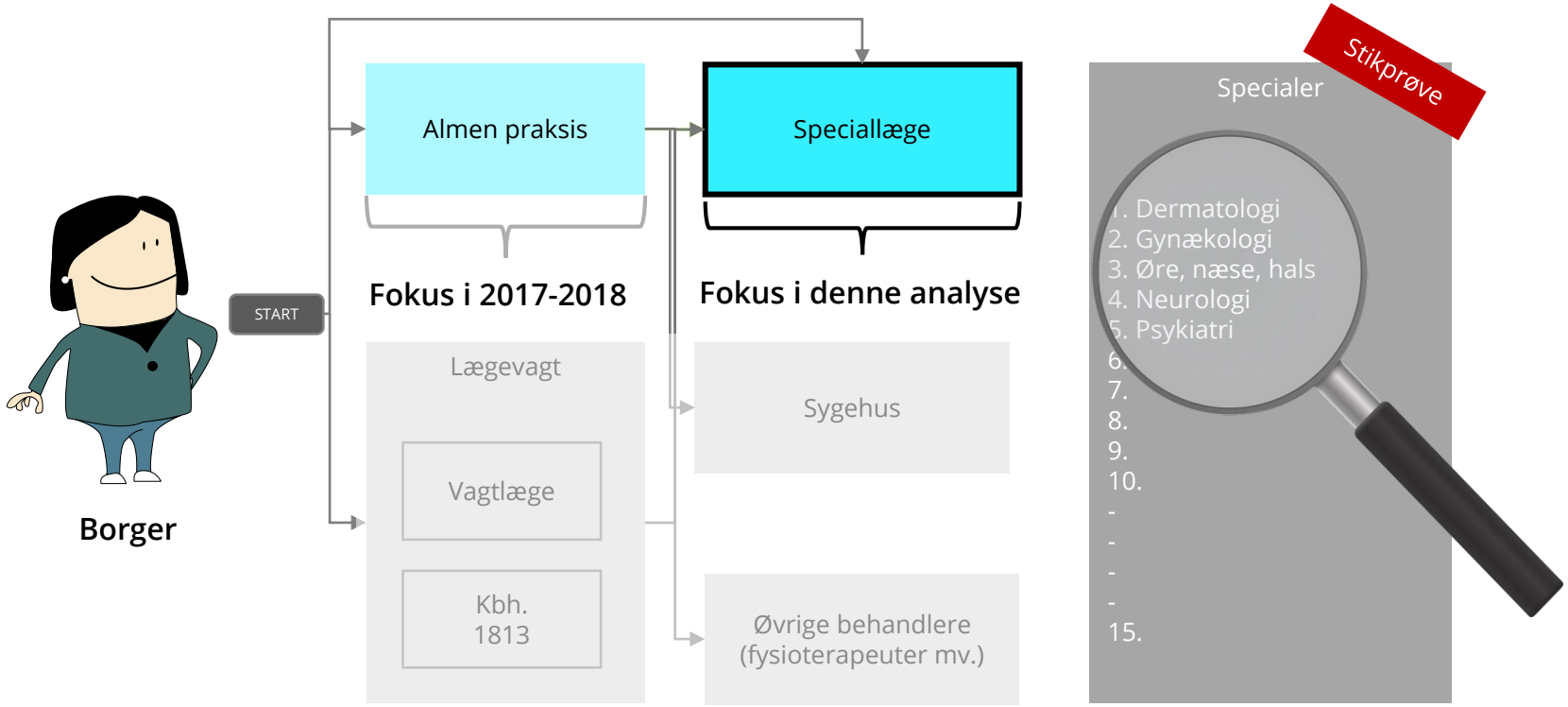
Udarbejdelsen af forbedringsforslag skal dog afspejle, at den dominerende model fortsat er små praksisser, som ikke har dedikerede ressourcer til informationssikkerhed. Den mindre klinik er kendetegnet ved relativt få ansatte, et mindre budget til it-sikkerhed og begrænset viden inden for it. Derfor er det anbefalelsesværdigt for klinikken at fokusere på de tiltag, der giver den størst mulige dækning sammenholdt med indsatsen. Deloitte har anvendt anbefalingerne fra Digitaliseringsstyrelsen i *Cyberforsvar der virker* samt de kritiske kontroller (CIS top 20), med fokus på basiskontroller målrettet små og mellemstore virksomheder.



# Speciallægens rolle i patientrejsen

Sundhedssektoren er som samfundskritisk sektor en integreret del af den nationale styringskæde for cyber- og informationssikkerhed. Opretholdelsen af et samlet set højt niveau af cyber- og informationssikkerhed i sundhedsvæsnet kræver, at der i alle led gennemføres de påkrævede foranstaltninger. Almen praksis var i 2017-2018 genstand for en analyse med særligt fokus på systemhusene, der i vid udstrækning er de samme som i speciallægepraksis. Nærværende analyse har fokus på speciallægerne og søger at komplementere den forrige analyse gennem **et mere klinik- og praksisnært fokus**.



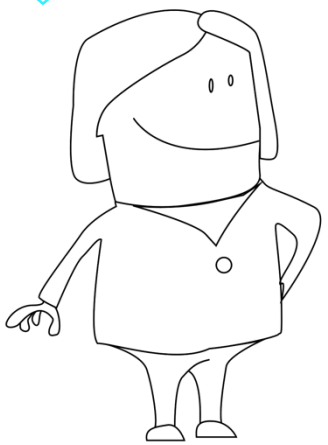
# Andre aktører i økosystemet

Foruden interviews med systemleverandører og speciallæger har andre væsentlige aktører været konsulteret: Praktiserende lægers organisation (PLO), MedCom (herunder Sundhedsdatanettet), Sundhedsdatastyrelsen (sektormyndigheden DCIS) og Region Sjælland (datakonsulent for almen praksis).

PRAKTISERENDE LÆGERS ORGANISATION

- Gode erfaringer med målrettede kampagner.
- Men det er en stor opgave, som kræver specialistviden og bør være bedre forankret nationalt.

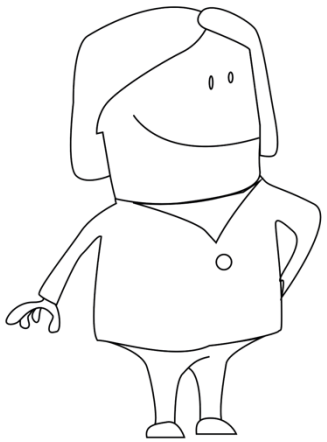
***PLO***



medcom

- Leverandørene er generelt afgørende for klinikkens informationssikkerhedsniveau.
- Flere aktører tror fejlagtigt, at sikkerhed (kryptering) håndteres i SDN-netværket

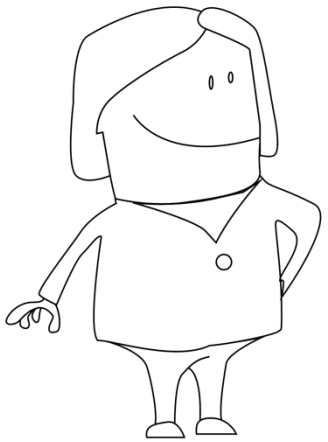
***MedCom***



SUNDHEDSDATA-STYRELSEN

- Mangler et risikobaseret overblik over landskabet med praksisser og andre private behandlere.
- Systemhusene burde forpligtes til at kunne modtage/håndtere sikkerhedsvarsler (MISP).

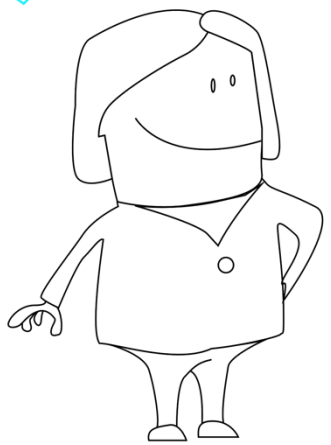
***DCIS (sektormyndighed)***



REGION SJÆLLAND

- It-hygiejne er en effektfuld måde at tale om informationssikkerhed med praksislægerne på.
- Lægerne har brug for konkrete og håndgribelige anbefalinger.

***Datakonsulent, Region Sjælland***



# Informationssikkerhed i de kliniknære arbejdsgange

En hverdag i klinikken består typisk af fem sekvenser, hvor de midterste – sekvens to til fire – gentages mange gange. Nedenstående illustrerer for hver sekvens sårbarheder, som den enkelte klinik særligt skal være opmærksom på.


## 1. Åbn klinik

Hos klinikkerne er det typisk den første, der møder ind, som tænder computerne. I to ud af seks klinikker står der i receptionen en tændt, ulåst computer uden opsyn, som er tilkoblet patientsystemet.

**I den ene klinik er det nødvendigt med en tændt computer, da denne er tilkoblet magnetscanneren. I den anden klinik anvendes computeren som radio i venteværelset.**

**I begge tilfælde udgør manglende opsyn og sikkerhed en forøget risiko for brud på informationssikkerheden.**


## 2. Patientankomst

I alle seks klinikker er der fokus på arbejdsgange med hensyn til GDPR.

Ingen klinikker har skærme, hvorpå patientens navn eller cpr-nummer står ved registrering på magnetscanner. I ingen af de besøgte klinikker er personfølsomme data blevet sagt højt i klinikken.

Der findes dog flere former for registrering i de seks klinikker. Nogle anvender en magnetstribe uden skærm, nogle anvender en magnetstribe med en skærm, og nogle har slet ingen maskine. **Ved glemt sygesikringsbevis skulle man i en enkelt klinik indtaste cpr-nummer på en skærm, hvorved de andre patienter i venteværelset i princippet kunne se det indtastede cpr-nummer.**

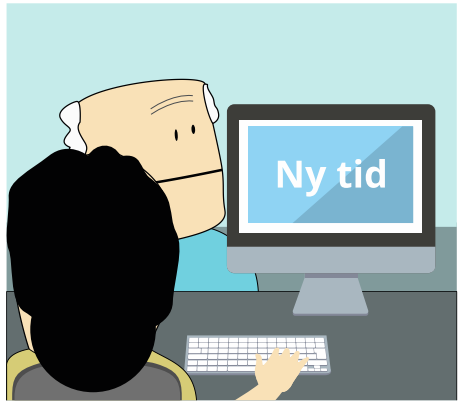
## 3. Patientkonsultation

De forskellige klinikkers konsultationsformer varierer. **Særligt én klinik anvendte meget medicoudstyr, hvoraf noget havde adgang til internettet.**

De fleste af klinikkernes konsultationer var samtalebaserede og anvendte lidt eller intet medicoudstyr (og ofte ikke koblet til nettet).

Ofte anvendte systemer/portaler er udover lægesystemet FMK, sundhed.dk, Webreq, Gmail, Hotmail og Google.

Lægen har i sit patienthåndteringssystem ikke adgang til hele patientens journal og sygehistorie: Lægen kan i første omgang se henvisning og egne noter. Når henvisningen er hentet, har lægen adgang til laboratoriesvar og medicinkort.




## 4. Ny tid

Efter endt konsultation bestilles der tid i receptionen. **Hos fire ud af seks klinikker var det muligt at se med på receptionistens skærm, da der ikke var installeret privacy-filtre eller anden beskyttelse.**

**Alle klinikker oplevede frustrationer ved fraværet af sikker mail, hvorfor mange anvender alternative mailsystemer.** Klinikkerne er opmærksomme på, at cpr-nummer samt andet personfølsomt data ikke skal indgå i mailen. Én klinik formodede at have sikker mail, men var ikke sikker.


## 5. Luk klinik

Efter endt arbejdsdag lukkes computere, arkivskabe samt klinik.

**Enkelte klinikker har fokus på at rydde skriveborde og tilsikre, at dokumenter med fortrolige informationer makuleres.**

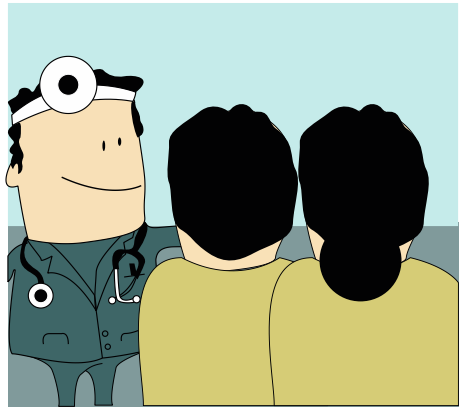
# Andre situationer hvor speciallægen skal være særligt opmærksom på informationssikkerhed

## A. Køb af hardware og lægesystem

Fire ud af seks speciallægeklinikker har købt al hardware gennem deres system-leverandør.

Udstyr, der kan være købt udenom system-leverandøren, er typisk printere og specialespecifikt udstyr, som system-leverandøren ikke tilbyder. **Flere speciallæger har udstyr koblet til internettet, hvilket udgør en unødvendig risiko for cyberangreb.**

Systemleverandøren vælges typisk på baggrund af anbefalinger fra netværk eller overtagelse fra tidligere klinikejer. Speciallægerne skifter sjældent systemleverandør, da det kræver meget tid at sætte sig ind i nye brugersystemer.



## B. Onboarding af personale

Fem ud af seks klinikker har ingen nedskrevet procedure for onboarding af personale.

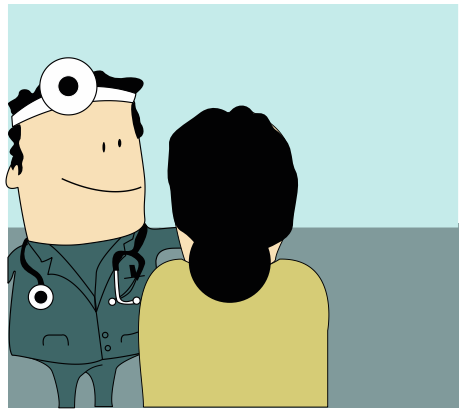
Klinikkerne består oftest af få ansatte med sjælden udskiftning, hvorfor klinikkerne oplever en nedskrevet procedure som værende overflødig. Kun én klinik havde en fysisk mappe med nedskrevne procedurer for onboarding med henblik på brugerlogin, arbejdsgange mv. **I flere tilfælde anvendes delte brugere og enkelte af disse med administratorrettigheder, hvilket markant øger risikoen ifm. cyberangreb.**

**Manglende awarenesstræning i forbindelse med opstart i klinikken kan have uheldige konsekvenser, fx i form af utilstrækkeligt fokus på håndtering af phishing/vishing og social engineering.**

## C. Andres adgang til klinikken

Alle klinikker havde ansat rengørings-personale. Disse havde nøgle til klinikken, men ingen adgang til hverken computer eller internet. Rengørings-personale har typisk fysisk adgang til klinikkens udstyr.

Andet personale, som typisk kan have adgang til klinikken, er sygeplejersker, lægesekretær, SOSU-assistenter, andre speciallæger, medicinstuderende og bogholdere.



## D. Offboarding af personale

Ligesom ved onboarding af personale havde fem ud af seks klinikker ingen nedskrevne procedurer for offboarding af personale.

Ved afsked med personale bliver bruger-adgangen enten lukket aktivt via eget system eller via systemleverandøren. **I nogle tilfælde lukkes brugeradgangen først, når kodeordet skal skiftes og ikke bliver fornyet.**

**I flere tilfælde anvendes der delte brugere, hvilket øger risikoen i forbindelse med et cyberangreb. Disse lukkes ikke i forbindelse med offboarding.**


## E. Beredskabsplan ved systemnedbrud

**Kun en klinik havde en nedskrevet beredskabsplan ved brud/angreb.**

**Klinikken havde her en fysisk mappe med en handleplan samt papirer/skemaer, som kunne hjælpe personale med fortsat at konsultere patienter ved systembrud.**

Ovenstående klinik er ligeledes den eneste klinik, som har opdaget, at de har været udsat for et hackerangreb.

**Hvis klinikken ikke har nedskrevne procedurer, udsættes klinikken for en unødvendigt høj risiko for tab af data som følge af cyberangreb.**

# Observerede sårbarheder på tværs af klinikker

Sårbarheder identificeret under besøg hos speciallægeklinikker er systematiseret i syv kategorier. Det skal bemærkes, at disse sårbarheder er dem, som det er muligt for speciallægerne og leverandørerne selv at påvirke. Senere i analysen vil tværgående forhold blive fremdraget som supplement hertil.

| | Mennesker | | | Processer | Teknologi | | |
|---|---|---|---|---|---|---|---|
| TEMAER | **Manglende kendskab til konsekvenser ved utilstrækkelig sikkerhed** | **Uklarhed om eget ansvar og krav til systemleverandør** | **Adgangsrettigheder og identiteter deles på tværs af personale** | **Manglende procedurer som fx beredskabsplaner og on- og off-boarding** | **Manglende sikkerheds-hærdning af it-udstyr** | **Utilstrækkelig adgangsstyring** | **Ikke-sikker korrespondance (bl.a. mail)** |
| | De praktiserende speciallæger er generelt opmærksomme på arbejdsgange og prøver at opsætte et sikkert miljø. På trods af dette er det i flere af klinikkerne muligt at tilgå fortrolige data, og der er generelt ikke tilstrækkelig kendskab til konsekvenser ved utilstrækkelig sikkerhed. | De praktiserende speciallæger har høj tillid til, at system-leverandøren leverer en optimal sikkerhedspakke, og de skifter sjældent leverandør. Flere steder er de nødvendige sikkerhedsforanstaltninger et tilkøb, som lægerne ikke har valgt til. | Flere af de besøgte klinikker deler brugeradgange /kodeord. I nogle tilfælde slettes adgange til afskediget personale først tre måneder efter fratrædelse. Dette giver et manglende overblik over adgange til fortrolige data. | De praktiserende speciallæger har generelt ingen nedskrevne procedurer om informations-sikkerhed. Særligt de, som scorer lavt på sikkerheds-barometret, stilles i en sårbar situation ved brud, da de hverken har hotline eller handleplan. | Hos flere af speciallægerne er der valgt en systemløsning hvor it-sikkerhed ikke er inkluderet i pakken. Herved er det speciallægens opgave selv at sikre "hærdning" (at holde systemerne opdateret mv.), hvilket giver en større risiko. | De fleste speciallæger arbejder ikke struktureret med it-adgangsstyring i journalsystem – og på (Windows) computeren, hvilket udsætter klinikken for risici i forhold til angreb og tab af data. | Alle speciallæger mangler en sikker mail til korrespondance med patienter, andre læger, forsikringsselskaber mv. Ligeledes savnes et system, hvori personalet i større klinikker nemt kan kommunikere internt og sikkert. |
| OBSERVEREDE SÅRBARHEDER | • Ubemandet og tilgængelig computer med adgang til EPJ<br>• Manglende privacy-skærme<br>• Lydt i klinikker (muligt at høre naborum, når patient sidder i venteværelset)<br>• Pc bliver ikke låst, når lokale forlades<br>• Åbne usb-porte<br>• Fysiske patientjournaler, der ikke ligger i aflåst skab<br>• Ulåst hardware (server)<br>• Arbejdscomputer anvendes til private formål<br>• Flere enheder er koblet op på internettet (særligt printere)<br>• Der gennemføres ikke træning | • Forventer at system-leverandør håndterer sikkerheden i systemet<br>• Der føres ikke tilsyn med systemleverandør<br>• Uklarhed om, hvad systemleverandør har leveret<br>• Tvivl om kontraktens indhold<br>• Ved ikke, om eget setup lever op til sikkerheds-standarder | • Brugerprofiler (kodeord) deles (også administrator-rettigheder)<br>• Mulighed for at rette/slette i journaler flere år tilbage<br>• Mulighed for at udskrive recepter<br>• Ingen/begrænset sporbarhed (der er et lovkrav om logning og muligheden for at føre opslag, ændringer mv. tilbage til den konkrete sundhedsprofessionelle) | • Manglende beredskabsplaner i tilfælde af angreb<br>• Ingen nedskrevne procedurer med fokus på sikkerhed ved on- og offboarding af personale | • Patch/sikkerheds-opdateringer forudsættes i nogle tilfælde foretage af lægen selv<br>• Backup og efterprøvning/test af backup foretages ikke<br>• Opsætning af firewall med relevante regler kræver it-indsigt, som speciallægen ikke nødvendigvis har | • Manglende opsætning af brugergrupper/brugere med passende rettigheder som afspejler jobfunktion<br>• For bred brug af administratorrettigheder<br>• Manglende rettidig lukning af adgange/profiler | • Mangler sikker mail og anvender derfor ofte Gmail eller lignende til at håndtere korrespondance.<br>• Personligdata kan fejlagtigt ligge i mailklienter, eller online løsninger, som ikke er lavet til dette (eksempelvis Gmail) |

# Variationer af sikkerhed blandt speciallæger

Databeskyttelse handler om mere end bare at implementere et sikkert it-system. Det handler om, hvordan databeskyttelse bliver tænkt ind i en virksomheds produkter, services, kultur og forretningsprocesser end-to-end. Der er konstateret en stor variation i sikkerhedsniveauet mellem de enkelte klinikker, og denne variation hænger sammen med hvilken grad af rådgivning, som lægerne har adgang til.

### En ulige tilgang til rådgivning

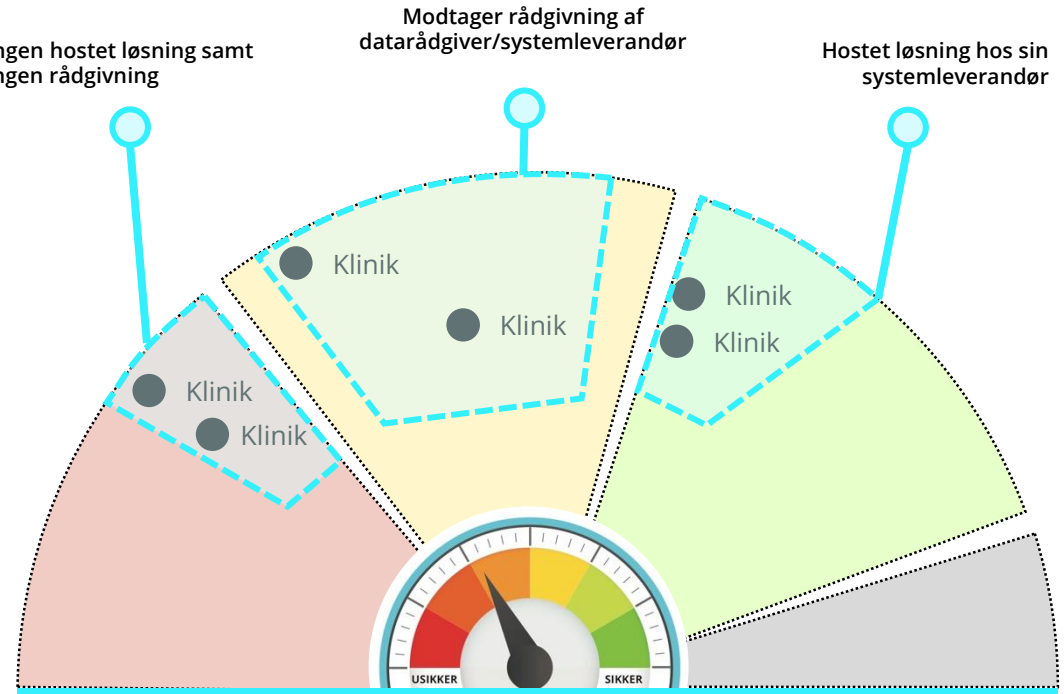
To ud af seks praktiserende speciallæger har en hostet løsning hos sin systemleverandør og anvender systemleverandøren som en hyppig sparringspartner til kliniknære anbefalinger. Her hjælper systemleverandøren med kliniknære anbefalinger samt tilbyder hjælp med indstillinger i systemet til for eksempel on- og offboarding af personale. Disse to klinikker scorede højest på sikkerhedsbarometret (se evt. forklaring heraf på side 33).

To ud af seks klinikker har anskaffet sig en datarådgiver udenom systemleverandøren for at få hjælp til at håndtere og forstå klinikkens informationssikkerhedsniveau. Den eksterne rådgiver giver kliniknære anbefalinger. Den ene af disse klinikker scorede middel på sikkerhedsbarometret, hvor den anden klinik scorede middel til lavt på sikkerheds-barometret.

To ud af seks klinikker anvender hverken systemleverandør som sparringspartner eller anden ekstern rådgiver med henblik på informationssikkerhed. Disse to klinikker scorede lavest på sikkerhedsbarometret.

Analysen sandsynliggør således, at der er en sammenhæng mellem sikkerhedsscore og adgangen til ekstern rådgivning. Denne observation er endvidere konsistent med 2019-analysen af små og mellemstore virksomheder.

Fire ud af seks af speciallægeklinikkerne har anskaffet sig supplerende ekstern rådgivning, de tre fra deres primære systemleverandør og én fra en ekstern datarådgiver.

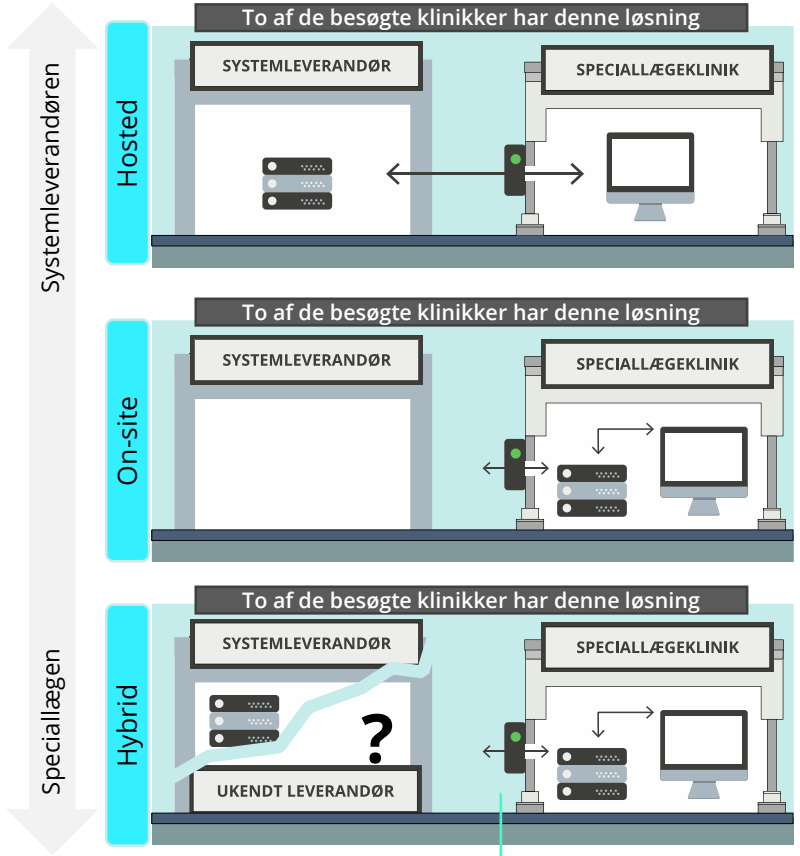



Klinikkens sikkerhedsniveau afhænger blandt andet af adgangen til rådgivning, som enten kan være fra systemleverandør eller anden ekstern rådgiver. Se også s. 33.

# Samarbejdet med systemleverandøren: et vigtigt valg for speciallægen

Et af de vigtigste valg, speciallægen skal tage i forhold til informationssikkerhed, er i hvor høj grad, systemleverandøren skal støtte klinikken med hjælp til informationssikkerhed. Skal klinikken selv have programserveren stående i klinikken, eller skal systemleverandøren varetage dette ansvar? Og hvad med eget indkøbt udstyr (printer og øvrigt udstyr) og generel sparring/hjælp til sikkerhed i klinikken? Hvis sikkerhedspakker samtidig fravælges, stiller et setup med eget vedligehold og/eller udstyr store krav til klinikken selv.




**1. Systemleverandøren vedligeholder programcomputeren**

Programserveren står hos systemleverandøren

- Løsningen indeholder oftest en sikkerhedspakke.
- Patches/opdateringer af systemer og infrastruktur foretages af leverandøren.
- Brugerstyring håndteres oftest hos systemleverandøren.
- Oftest foretager leverandøren udvidet sikkerhedsvejledning.
- Systemleverandøren foretager oftest konfiguration af firewall og lokal firewall på computeren.
- Leverandøren stiller oftest antivirus/malware til rådighed og monitorerer udstyr i forhold til sikkerhedsbrud.

**2. Speciallægen vedligeholder programcomputeren**

Server står i klinikken, men alt udstyr er købt af systemleverandør

- Når programserveren stilles fysisk hos den enkelte klinik, introduceres flere risici.
- Indeholder normalt ikke en sikkerhedspakke (ekstra)
- Adgangsstyring foretages oftest af klinikken selv.
- Vedligehold/patching af udstyr foretages af klinikken.
- Konfiguration af hardware, herunder for eksempel firewall/router, forventes foretaget af klinikken selv.

**3. En kombination, hvor speciallægen har indkøbt udstyr udenom systemleverandøren (eksempelvis printer eller lignende)**

Speciallægens server står i klinikken; ikke alt udstyr er købt af systemleverandør

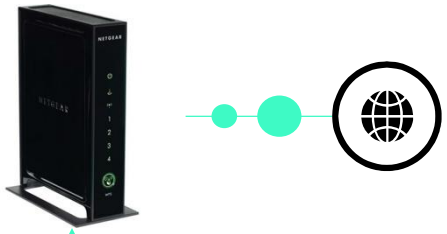
- De samme krav til speciallægen som i eksempel 2.
- Egetindkøbt udstyr stiller øgede krav til speciallægen, hvis der ikke er købt udvidet support (hos eksempelvis systemleverandøren).
- Klinikken sørger for at patche og opdatere eget udstyr.
- Klinikker i respondentgruppen indser oftest ikke, hvilken risiko det indebærer at have egetindkøbt udstyr, uden på tilsvarende vis at have en plan for sikring og vedligehold (eksempelvis udvides angrebsfladen væsentligt, når printere tilgår internettet).

### Vigtigt om modem/router

Klinikkens valg af internetudbyder (ISP) og leverandørens løbende vedligehold af klinikkens udleverede udstyr (sikkerhedsopdateringer) er vigtigt at være bevidst om.

Klinikkens modem/router er den enhed, der forbinder klinikken med internettet. Der bør være løbende sikkerhedsopdateringer af denne enhed, og enheden bør sikkerhedskonfigureres for at modstå angreb fra internettet.

*Dette er oftest en del af systemudbyderens sikkerhedspakke (typsik ekstra tilkøb).*



# Gensidig usikkerhed om passende foranstaltninger

Analysen viser, at både speciallæger og systemleverandører mangler minimumskrav eller på anden måde en fælles forståelse af passende foranstaltninger til at rammesætte samarbejdet. Systemleverandørerne efterlyser på den ene side minimumskrav for hvordan, de praktiserende speciallæger lever op til informations-sikkerhedsmæssige anbefalinger. Ligeledes mangler den praktiserende speciallæge på den anden side en praktisk anvendelig fortolkning af lovkravet om "passende foranstaltninger", hvilket eksempelvis kunne være minimumskrav til systemleverandøren.

# Systemleverandørerne savner sektorspecifikke anbefalinger om informationssikkerhed

Enkelte leverandører viser vejen med informationssikkerhed som konkurrenceparameter, men sektoren bør udstikke fælles vejledende anbefalinger, som kan rammesætte dialogen med speciallægerne.

**Vi har spurgt seks leverandører af journalsystemer til deres tilgang til informationssikkerhed og deres oplevelse af dialogen med speciallægerne**

Respondentgruppen består af seks lægesystemleverandører. Disse systemer er valgt af 92 % af speciallægerne (oversigt fremgår af s. 31). Der var en forventning om, at større leverandører ville have mere fokus på informationssikkerhed – både i interne processer, men også i systemudvikling. Dette ud fra en vurdering af, at de større leverandører har flere ressourcer til at prioritere dette område, og fordi de større leverandører ofte leverer ydelser til andre brancher, hvor informationssikkerhed efterspørges. Analysen viser imidlertid ikke denne sammenhæng: Modenheden i processerne omkring informationssikkerhed er ikke betinget af leverandørens størrelse. Til gengæld har analysen vist, at enkelte systemudbydere begynder at lade sig certificere og særligt i årsrapporten og lignende gør opmærksom på deres fokus på informationssikkerhed.

En ændret prioritering af tiltag vedr. informationssikkerhed hos systemleverandøren, også som opfølgning på Ezenta-rapporten om almen praksis, vurderes at kunne skabe et bedre fundament for sikker it-udvikling og ultimativt et mere sikkert produkt til glæde for såvel praksisser som borgere.

**Observation 1: Dialogen om informationssikkerhed opleves til tider som "mersalg"'**

Der eksisterer ikke på nuværende tidspunkt en ensretning i forhold til sektorens prioritering af informationssikkerhed (ingen anbefalinger fra branchen eller relevante interesseorganisationer). Det betyder, at dialogen let opfattes som et salgsmøde, da:

- Dialogen bliver præget af personlige holdninger og begrænset forståelse for it hos speciallægen (speciallægen er ganske enkelt ikke klædt fagligt godt nok på til diskussionen om informations-sikkerhed)
- Det er op til den enkelte speciallæge at prioritere arbejdet med informationssikkerhed og herved opnå et "passende informationssikkerhedsniveau" – hvilket for mange opleves som en abstrakt fortolkningsøvelse, der ikke er støttet af konkret vejledning.

**Observation 2: Der er brug for sektorspecifikke anbefalinger**

Analysen viser – set fra begge parters side – at et sæt sektoranbefalinger vil hjælpe i dialogen. Speciallægen kan henvise til disse anbefalinger, og systemleverandøren kan fokusere på dialogen med henvisning til disse anbefalinger. Det sundeste for dialogen og den samlede sikkerhed vil være konsensus om anbefalede minimumskrav, som systemleverandørerne begynder at arbejde konkurrencefokuseret med og derfor vælger at prioritere i produkterne på egen hånd.

**Sikkerhed som konkurrenceparameter: nogle få viser vejen**

- Leverandørens størrelse er ikke afgørende for graden af investering/fokus på it-sikkerhed.
- To ud af seks af leverandørerne er ISO 27001-certificerede, hvilket sender et signal om, at sikkerhed er en særlig prioritet i organisationen for de pågældende to leverandører.
- Alle leverandører tilbyder (eller vil kunne tilbyde) en løsning, hvor it-sikkerhed er inkluderet i prisen. Det kaldes en "hosted løsning", hvor leverandøren sørger for infrastrukturen. Denne løsning er derfor dyrere.
- Løsningen hvor speciallægen selv skal stå for sikkerheden, kaldes en on-premise- løsning og betyder, at it-sikkerhed er et tilkøb eller noget, klinikken selv skal stå for.
- Når it-sikkerhed ikke er inkluderet i prisen, oplever leverandørerne, at dialogen med speciallægerne er udfordret og ofte bliver set som forsøg på mersalg.
- Forståelsen af et "passende informationssikkerhedsniveau" er individuel og ikke forankret i et brancheanerkendt niveau.

Det er Deloittes vurdering, at hvis der etableres sektorspecifikke minimumanbefalinger, vil systemhusene begynde at anvende disse som konkurrenceparametre, og disse minimumanbefalinger vil ligeledes kunne være underlagt revision (det bliver herved samtidig muligt at lægge dem til grund for tilsyn).

# Kliniknære anbefalinger

Ni konkrete tiltag til forbedring af it-sikkerheden i klinikken. Mange af dem vil med fordel kunne løftes eller understøttes på tværs af de enkelte praksisser.

Ved besøgene udviste klinikkerne generelt en høj bevidsthed og et ønske om beskyttelse af personfølsomme data, særligt grundet erfaringer med GDPR-krav. Til gengæld var viden om tekniske foranstaltninger og generel informationssikkerhed (foruden fortrolighed også integritet og tilgængelighed) i langt mindre grad i fokus end de mere juridiske krav. En hypotese om at klinikkerne køber meget udstyr selv blev delvist afkræftet; klinikkerne benytter i udstrakt grad også leverandøren til udstyr, som leverandøren dermed også har et medansvar for.

En fællesnævner hos alle besøgte klinikker var et højt niveau af tillid til systemleverandøren, patienter, pårørende og personale. Dette er i mange sammenhænge en positiv tendens, men ud fra en informationssikkerhedsmæssig risikobetragtning anbefales det at anlægge en mere skeptisk tilgang. Kriminelle *kan* potentielt udnytte den danske mentalitet. De praktiserende speciallæger var alle opmærksomme på egne arbejdsgange i klinikken, således at de ikke selv lavede fejl. Ingen overvejede dog udefrakommende kriminelle eller andre med interesse i data. Dette er en sårbarhed, som let kan udnyttes.

Der eksisterede ikke sektorspecifikke anbefalinger for it-sikkerhed på tidspunktet for denne analyse, hvilket betyder, at det er op til klinikken at vurdere nødvendigheden (eller manglen på) af informationssikkerhed. Det udfordrer dialogen med systemleverandøren. For en mindre klinik med få ansatte er det særligt vigtigt at *fokusere* på de få tiltag, som virker, med henblik på at få den største grad af beskyttelse for de prioriterede tiltag. Flere af konklusionerne fra 2017-analysen af almen praksis (Analyse af praksissektorens systemhuse (2017, med opfølgning i 2018)) kan videreføres til speciallægepraksis. Dog består en speciallæge-praksis oftest af få ansatte, hvorved prioritering af tiltagene i forbindelse med informationssikkerhed oftest sker med konsekvens for andre aktiviteter i klinikken. De fleste deltagende speciallæger er udfordrede på at forstå kontrakten med systemleverandøren og på at forstå det tekniske setup med journalsystem og infrastruktur. Hos de udvalgte seks klinikker var det tydeligt, at klinikker, som havde et tæt samarbejde med systemleverandøren, også har et styrket sikkerhedsniveau. De var blevet vejledt af deres leverandør i forhold til sårbarheder med udgangspunkt i egen klinik og havde en dialog omkring typiske sårbarheder i klinikken.

I nogle besøgte klinikker var der en overbevisning om, at sikkerhed er udliciteret til leverandøren og dermed er dennes ansvar. Det er ikke rigtigt; speciallægen er dataejer og har i sidste ende det fulde ansvar selv. Lægen kan kræve, at leverandøren lever op til "passende sikkerhedsforanstaltninger", men ikke uden selv at implementere leverandørens anvisninger/anbefalinger.

**Kliniknære anbefalinger til forbedring af informationssikkerheden**
Se også s. 42, hvor de er omsat til en klinikvendt poster. Se derudover den generelle værktøjskasse s. 41.

1. **Sørg for klare aftaler om ansvar og arbejdsdeling med systemleverandøren** og sørg for at forstå de kontraktlige forhold – herunder databehandleraftalens krav om kryptering af trafik til og med SDN-knudepunktet samt aftalens dækning af it-sikkerhed (backup, konfigurering mv.).
2. **Etablér en serviceaftale for informationssikkerhed:** Etablér en serviceaftale ekstern part, som klinikken kan ringe efter hjælp i tilfælde af angreb eller nedbrud – flere systemleverandører tilbyder fx selv denne service.
3. **Opsæt informationsmateriale og træn awareness.** Opsæt fx visuelle virkemidler, så informationssikkerhed bliver en naturlig del af hverdagen. Overvej periodiske awarenessforløb.
4. **Udarbejd en intern beskrivelse af klinikkens it-hygiejne** (inden for forhold som håndtering af patientoplysninger, password, håndtering af usb, brugen af sikker mail mv.).
5. **Tag stilling til håndtering af nødsituationer og til brugernes adgange**: Udarbejd procedurer for beredskab (nødplaner) samt brugerstyring, så den ønskede adfærd gøres konkret.
6. **Tjek klinikkens backupaftale** med henblik på, hvorvidt alt relevant data kan genetableres.
7. **Begræns opkobling af udstyr på internettet** (eksempelvis printere) og påse tilstrækkelig fysisk sikring af udstyr.
8. **Få foretaget en årlig sårbarhedstest af klinikkens it-miljø** (antivirus, firewall, porte er blokerede, netværksadgange lukkede, gamle brugeradgange er lukket ned, harddiske er krypterede) og få i denne forbindelse en årlig træning i it-/informationssikkerhed.
9. **Sørg for sikker kommunikation med patienter**; flere systemleverandører stiller for eksempel portaler til rådighed som en del af samarbejdsaftalen.

> ***"Jeg er en dygtig læge. Jeg er ikke uddannet i it. Jeg forstår ikke det sprog. Derfor betaler jeg mig fra det, og så må jeg håbe, at min leverandør har styr på det."***
> *Praktiserende speciallæge*

# Leverandørvendte anbefalinger

Syv konkrete tiltag til forbedring af informationssikkerheden i klinikken igennem forbedret samarbejde med systemleverandøren.

### Systemleverandøren er speciallægens sparringspartner

Analysen viser, at systemleverandørens rådgivning er en central del af klinikkens vidensgrundlag. Men analysen har samtidig vist, at der er en gensidig usikkerhed omkring passende foranstaltninger og anbefalede minimumskrav, som aktuelt vanskeliggør dialogen. På tidspunktet for udarbejdelse af denne rapport er der som følge af sektorstrategiens indsatsområde vedr. krav til leverandører opstartet en dialog mellem flere parter i sektoren med henblik på bl.a. at udarbejde et sæt anbefalinger til journalsystemer. Deloitte forventer derfor som følge af denne dialog, at sektoren vil blive enige om nogle systemmæssige anbefalinger, som vil foreligge i 2021.

### Manglende fælles forståelse for 'passende it-sikkerhed'

Det er Deloittes vurdering, at systemleverandørerne og speciallægernes forskellige forståelse af et "passende it-sikkerhedsniveau for speciallæger" hovedsageligt bunder i det manglende fælles udgangspunkt. Igennem vores interviews blev det klart at

- Dialogen omkring informationssikkerhed udfordres af at speciallægen, i den lille praksis, oftest ikke selv har kompetencerne og forståelsen for informationssikkerhed til at vurdere hvad, der er nødvendigt og hvad, der ikke er nødvendigt ift. sikkerhedsmæssige tiltag
- Samtlige leverandører tilbyder rådgivning om informationssikkerhed, men oplever, at dialogen opfattes som mersalg, da speciallægen har fokus på, at de alene behøver et journalsystem
- De manglende sektorspecifikke minimumsanbefalinger betyder, at dialogen mangler en fælles forståelsesramme

### Systemleverandøren bør ikke vente på minimumsanbefalingerne, men allerede nu indgå i dialog med speciallægerne

Som følge af analysens konkrete observationer fra interviews med systemleverandører, speciallæger og datakonsulenten fra Region Sjælland, anbefales det, at der allerede nu okuseres på at lukke identificerede sårbarheder og forbedre samarbejdet parterne imellem. Dette bør foretages med udgangspunkt i den nuværende service/kontrakt sammenholdt med rapportens anbefalinger.

Informationssikkerhed er i dag som udgangspunkt en ekstra ydelse fra systemleverandørerne. Systemleverandøren har her en særlig opgave med at få forklaret det kontraktuelle grundlag, herunder særligt punkterne omkring (manglende) it-sikkerhed i forhold til roller og ansvar.

**Leverandørvendte anbefalinger til forbedring af informationssikkerheden**

1. **Gennemgå kontrakten sammen med speciallægen:** Kontakt speciallægen med henblik på gennemgang af kontrakten, så roller og ansvar ifbm. informationssikkerhed i det nuværende forhold forstås og anerkendes af begge parter
2. **Indtag en sparrende rolle over for speciallægen:** Gennemgå eksempelvis særligt kritiske forhold, såfremt speciallægen ikke er dækket af den eksisterende aftale (backup og genetablering, policy-styring, brugerstyring, password, patch og konfigurering, firewall samt anti-virus/malware)
3. **Tilsikr at data er krypteret i journalsystemet:** Region Sjællands datakonsulent erfarer at flere, især ældre versioner, ikke er krypteret hvilket udgør en stor sårbarhed ift. et angreb (kendskab til ældre systemer, som ikke er patchet bør kommunikeres til speciallægen)
4. **Tilsikr at forbindelsen til SDN-knudepunktet er krypteret,** herunder også forbindelsen mellem systemleverandøren og speciallægen (VPN). Vær proaktiv ift. evt. mangler i databehandleraftalens krav omkring dette forhold.
5. **Tilbyd sårbarhedsscanninger** som grundlag for en konkret anbefaling om at lukke identificerede sårbarheder
6. **Indgå dialog med speciallægen omkring en teknisk forsvarlig løsning til kommunikation med patienter** (fx en portal hvor historik gemmes og hvor kommunikationen er krypteret). Patienter forventer en høj grad af fortrolighed i behandling af forespørgsler og udveksling af information, bl.a. som følge af GDPR
7. **Anse styrkelse af interne processer for it-sikkerhed som et konkurrenceparamete**r. Dette vil komme mere i fokus i fremtiden: Overvej mulig certificering ift. et anerkendt it-sikkerhedsmæssigt rammeværk som eksempelvis ISO 2700X.

> ***"Jeg oplever ikke, at speciallægen efterspørger it-sikkerhed. Når vi åbner dialogen omkring sikkerhed, opleves det oftest som et forsøg på mersalg. Det er ærgerligt."***
> *Systemleverandør*

# Tværgående anbefalinger

Otte anbefalinger til forbedring af informationssikkerheden på det tværgående niveau.

De tværgående anbefalinger skal ses i sammenhæng med erfaringerne fra PLO og SUMs fælles indsats for styrket it- og informationssikkerhed i almen praksis. Derudover skal de ses i sammenhæng med sektorstrategiens indsatsområde vedr. leverandørkrav og det igangværende tværgående arbejde med at definere fælles mindstekrav, som samtidig vil sætte rammerne for en del af de øvrige anbefalinger. Anbefalingernes økonomiske konsekvenser er ikke opgjort, men bør belyses parterne imellem og kan for nogles vedkommende eventuelt ses i sammenhæng med overenskomstforhandlingerne.

1. Udbyg og målret sikkerdigital.dk: Portalen bør – som også anbefalet i SMV-analysen fra 2019 – udbygges med målrettede og konkret handlingsanvisende vejledninger, der er relevante for de praktiserende speciallæger. PLOs awarenessunivers kan i samme forbindelse indarbejdes på og vedligeholdes samlet under sikkerdigital.dk. I sammenhæng hermed er det væsentligt, at der er entydighed omkring hvad, den autoritative kilde til rådgivning om retningslinjer, trusler og forholdsregler er, herunder væsentligt at DCIS' kanalstrategi og arbejdsdelingen med såvel regionerne som FAPS/PLO afklares. Det anbefales endvidere, at speciallægepraksis deltager i DCIS' kommende beredskabsøvelser.

2. Understøt klinikkerne med informationstiltag: Det anbefales, at der fra centralt hold (fx DCIS) gennemføres informationstiltag som awarenesskampagner, vejledningsmateriale mv.

3. Etabler en entydig indgang til rådgivning: Der bør etableres en generel ordning, som giver klinikkerne adgang til kontekstspecifik rådgivning, awareness og evt. tillige gennemgang af udstyr og arbejdsgange, fx gennem periodiske besøg i klinikken. Samme ordning kan bruges til at sikre, at tilsynsrapporterne fra leverandørerne til de enkelte læger bliver gennemgået. Der kan ved etableringen af ordningen ses på de positive erfaringer med regionale datakonsulenter i almen praksis. Det vil være centralt, at der er tale om en betroet instans med en kontinuert relation til sektoren (så der opbygges viden, erfaringer og tillid), jf. det kortlagte problem med at leverandørernes anbefalinger bliver set som forsøg på mersalg. Det bør i sammenhæng hermed afklares, hvordan klinikkerne får adgang til 24/7 operationel rådgivningsservice, herunder akut.

4. Udstik anbefalede minimumsstandarder for sektoren: For at adressere den gensidige usikkerhed mellem klinik og leverandør om passende foranstaltninger bør der defineres anbefalede minimumsstandarder. Dette bør være en myndighedsopgave, og på tidspunktet for analysens gennemførsel var et sådant initiativ i gang nationalt. Det anbefales at afstemme med nærværende analyse, herunder at opnå fælles forståelse for hvilke af de øvrige anbefalinger, som minimums-standarderne også understøtter (dette vil nemlig afhænge af hvordan, de udformes).

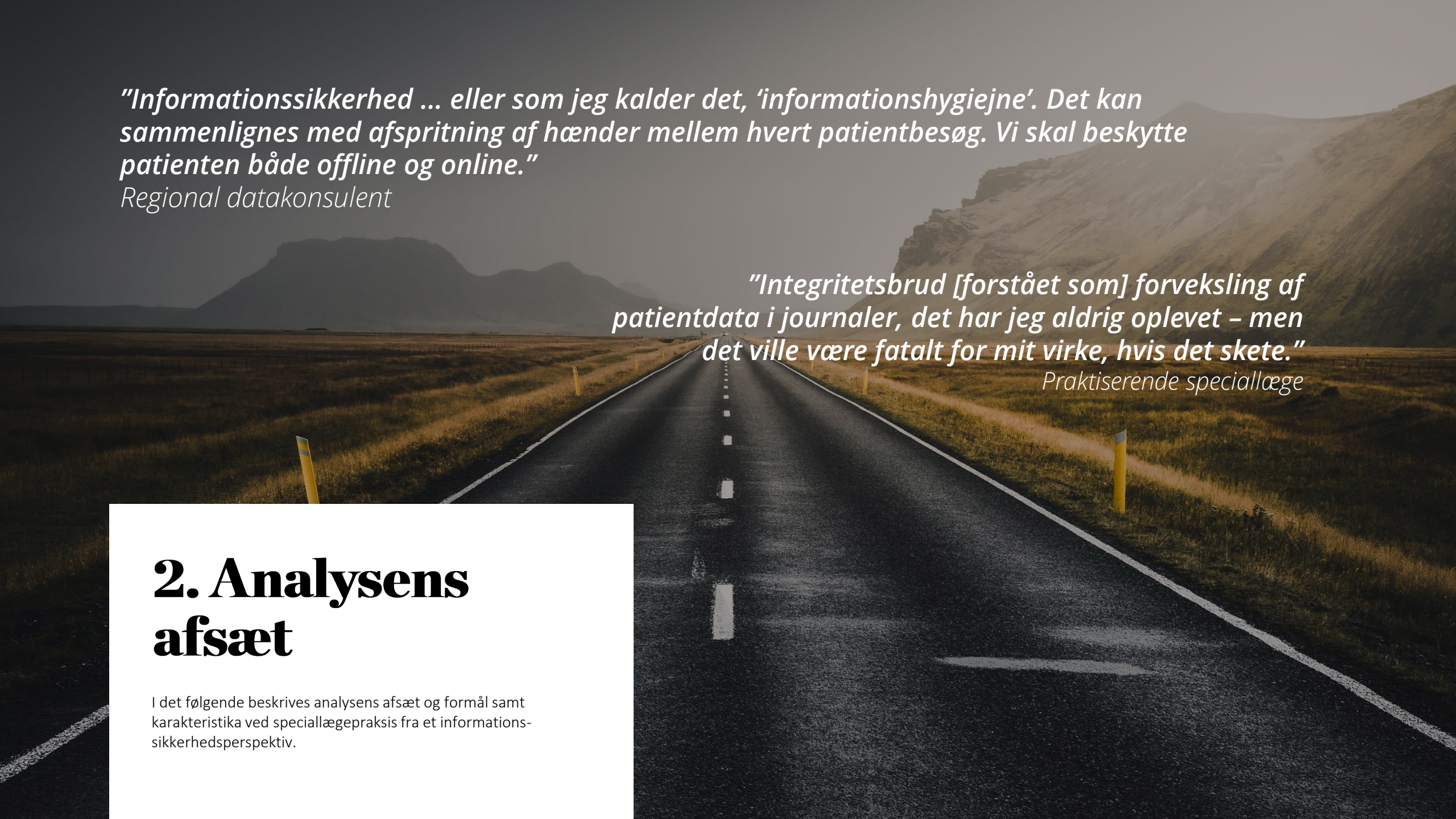
5. Udbred sikker mail: Flere klinikker udtrykker frustration over ikke at have en sikker mail-løsning, når der kommunikeres med patienter. Ofte kommunikeres med eksempelvis Gmail og øvrige løsninger, hvor der ikke nødvendigvis indestås for kryptering. Som et tværgående initiativ bør det tillige overvejes, hvorvidt portaler eller tilsvarende løsninger kan stilles til rådighed.

6. Aftal hændelseshåndtering med systemleverandørerne: Systemleverandørerne bør forpligtes på at kunne modtage og reagere på sikkerhedsvarsler fra sektormyndigheden DCIS' MISP-service.*

7. Analyse af forbundet medicoapparatur: Der bør i sammenhæng med sektorstrategiens udmøntning generelt gennemføres en analyse af de særlige cyber- og informationssikkerheds-mæssige risici forbundet med medicoteknisk apparatur (særligt hvis det er på nettet og fx har ekstern adgang til servicering mv.) og hele medico-IoT-økosystemet. I denne forbindelse bør der også opstilles målrettede anbefalinger til speciallæger med medicoteknisk udstyr.

8. Kræv kryptering på Sundhedsdatanettet og afklar ansvar for databehandleraftaler på tværs: Det er en udbredt fejlopfattelse, at data beskyttes gennem kryptering på Sundhedsdatanettet (SDN). Den enkelte leverandører skal imidlertid selv sikre den fornødne kryptering. Praksissektorens standarddatabehandleraftaler med systemhusene bør således have indskrevet krav om kryptering af data op indtil overdragelse af data på SDN-knudepunktet. Endvidere bør ansvaret for databehandleraftaler for datatrafikken på tværs af netværkets aktører afklares.

*) I det omfang den enkelte praksis selv har ansvar for lokalt maskineri (pc, servere) vil det dog ikke være tilstrækkeligt alene at kontakte leverandøren), jf. beskrivelsen ovenfor af forskellige modeller for hvilken service, lægen køber af leverandøren.



*”Informationssikkerhed … eller som jeg kalder det, ‘informationshygiejne’. Det kan sammenlignes med afspritning af hænder mellem hvert patientbesøg. Vi skal beskytte patienten både offline og online.”*
*Regional datakonsulent*

*”Integritetsbrud [forstået som] forveksling af patientdata i journaler, det har jeg aldrig oplevet – men det ville være fatalt for mit virke, hvis det skete.”*
*Praktiserende speciallæge*

# 2. Analysens afsæt

I det følgende beskrives analysens afsæt og formål samt karakteristika ved speciallægepraksis fra et informations-sikkerhedsperspektiv.

# Analysens afsæt og formål

Analysens hovedformål er at komme med praksisnære anbefalinger, der er både handlingsanvisende og helhedsorienterede. Da der allerede foreligger analyser af henholdsvis leverandører til almen praksis og af cyber- og informationssikkerhed i SMV'er, vil hovedfokus derfor være på at forstå vilkår og muligheder med afsæt i det daglige, herunder hvilke betingelser speciallægerne og Foreningen af Praktiserende Speciallæger (FAPS) har for at adressere leverandørsikkerheden.

Sundheds- og Ældreministeriet har sammen med FAPS og Danske Regioner ønsket at gennemføre en analyse af cyber- og informationssikkerheden blandt speciallæger. Analysen skal bygge videre på eksisterende analyser og skal munde ud i konkrete forbedringsforslag.

**Baggrund og sammenhæng med strategier**

En effektiv udmøntning af sektorstrategien for cybersikkerhed forudsætter, at der i alle kædens led er grundlag for at opretholde en passende sikkerhed og i det daglige arbejde udvise den rette adfærd. I 2018 blev der således i strategien for digital sundhed formuleret et mål om en bredere indsats på praksisområdet:

> Indsatsen for informationssikkerhed i praksissektoren handler om en bredere indsats for sikkerhed, bl.a. organisering af sikkerhedsarbejdet, adfærd, fysiske forhold og arbejdsgangene for behandling af sundhedsdata og personlige oplysninger. Der skal derfor sikres øget opmærksomhed på cyber- og informationssikkerhed på praksisområdet med bl.a. kampagner for øget opmærksomhed blandt lægerne på informationssikkerhed.

Tilbage i efteråret 2017 iværksatte Sundheds- og Ældreministeriet og PLO en indsats rettet mod sikkerhed i almen praksis, der identificerede en række udfordringer, herunder vedrørende leverandørsikkerheden. Da selv store organisationer har udfordringer med leverandørstyring, må det forventes, at sådanne forhold i væsentlig grad skal adresseres på tværgående niveau.

**Bidrag til kumulativ videnopbygning**

Analysen skal i relevant omfang bygge videre på allerede foretagne analyser og opnåede erfaringer. I den forbindelse kan særligt to analyser fremhæves:

1) Analyse af praksissektorens systemhuse (2017, Ezenta for PLO), hvor nærværende analyse vil argumentere for, at konklusionerne også gælder speciallægepraksis.
2) Analyse af små og mellemstore virksomheders (SMV'er) behov for informationsudveksling om IT-sikkerhedshændelser (2019, Deloitte for Erhvervsstyrelsen), hvor følgende konkluderes:

   *"[SMV'erne] efterspørger **målrettede vejledninger og værktøjer** (…) De efterspørger vejledning om **styring af deres IT-sikkerhedsleverandører**, så de kan ramme den rigtige balance mellem risiko og omkostninger. (…) [Det anbefales, at] eksisterende vejledninger og værktøjer, hvor det er hensigtsmæssigt, revideres, så de afspejler de forskellige situationer og udgangspositioner, som SMV'erne kan befinde sig i, og anvender **cases og brugerrejser som centrale designprincipper**."*

Med denne ansats har nærværende analyse såvel i sit design som i sit output fokus på netop det praksisnære. Der har undervejs i arbejdet løbende været dialog med den sektoransvarlige myndighed (DCIS) i Sundhedsdatastyrelsen med henblik på at sikre, at analyse og anbefalinger er afstemt med og bidrager til porteføljen af initiativer under sektorstrategien.

# Speciallægepraksis og almen praksis

Speciallægepraksisområdet dækker 15 forskellige specialer med betydelig indbyrdes forskelle i forløb og relation til patienterne. I et informationssikkerhedsperspektiv er der dog væsentlige sammenfald mellem almen praksis og speciallægepraksis, og særligt de fælles systemleverandører giver et fælles grundlag på tværs af praksissektoren.

### Patientrelation, patientforløb og kodepraksis har fællestræk med sygehuse

Speciallægepraksis minder på nogle områder mere om sygehuse end om almen praksis. Eksempelvis hvad angår faglig specialisering, patientforløb og registreringspraksis. Mange speciallæger har en baggrund som sygehuslæger, og anvender oftere specialiseret udstyr og endvidere samme kodesprog som på sygehusene (ICD-10).

I et informationssikkerhedsperspektiv er det særligt patientforløbene og nogle specialers anvendelse af medicoteknisk apparatur, som adskiller speciallægerne fra lægerne i almen praksis. Der er ved udvælgelsen af specialer søgt at tage højde herfor. Endvidere er der speciallæger (for eksempel anæstesilæger), som ikke har egen klinik og i stedet leverer en specialistservice til en anden klinik.

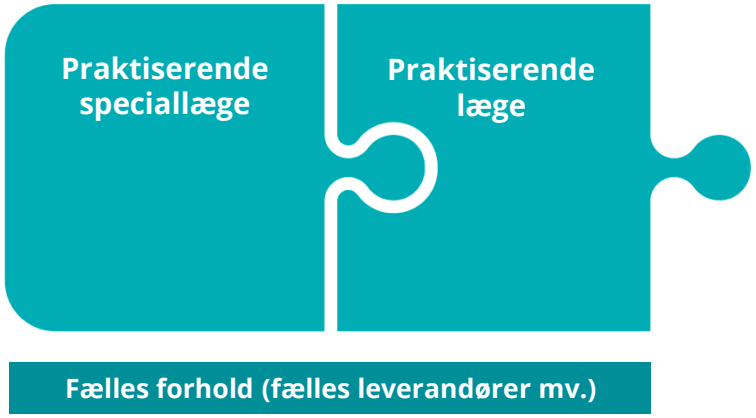
### I et informationssikkerhedsperspektiv er der dog væsentlige fællestræk med almen praksis

Omvendt er der på en række andre områder væsentlige ligheder mellem praksisklinikker og speciallæger. Fra et informationssikkerhedsmæssigt perspektiv kan særligt tre forhold fremdrages:

1. Der er i overvejende grad tale om små virksomheder, som af samme grund sjældent har specialistviden inden for it og informationssikkerhed.
2. Der er på leverandørsiden et stort overlap mellem speciallægepraksis og almen praksis, og langt hovedparten af klinikkerne har leverandører organiseret i det fælles PL-forum (se tabel med oversigt over leverandørerne i Bilag).
3. Begge er primærsektor og med regionerne som myndighedsansvarlige.

Kombinationen af de to første punkter er særligt væsentlig: Små virksomheder vil ofte lægge sig op ad deres it-leverandørs processer, og da de fleste klinikker har leverandører, som også servicerer almen praksis, må det som udgangspunkt forventes, at leverandørrelaterede risici i almen praksis også er relevante for speciallæger. Endvidere tilbyder systemhusenes organisering i et leverandørforum en fælles struktur for koordinering og tværgående tiltag.

*Lighederne mellem almen praksis og speciallæger gør såvel denne analyse som den tidligere i almen praksis relevante for den samlede praksissektor.*



*"Hvem skal jeg stole på? Jeg er ikke god til it. Jeg tænkte, at jeg havde betalt mig fra det gennem min leverandør."*
*Praktiserende speciallæge*

*"Vi tænker hele tiden over informationssikkerhed; det er indlejret i frontallappen."*
*Praktiserende speciallæge*

# 3. Tilgang og metode

I dette afsnit gøres der rede for analysens metodiske ramme samt de aktiviteter, der er gennemført ved dataindsamlingen.

# Tilgang til analysen

**En praksisnær analyse af speciallægens hverdag og samarbejde med systemleverandøren. Analysen kombinerer etnografisk metode med en kontrolbaseret tilgang til informationssikkerhed.**

Formålet med analysen er at udarbejde konkrete forslag til forbedring af informationssikkerheden hos speciallæger. Alle klinikbesøg blev udført af et team med henholdsvis en etnograf og en cyber- og informations-sikkerhedsekspert. Herved kunne den sikkerhedsfaglige ekspertise kombineres med de mere etnografiske indsigter i brugeradfærd.

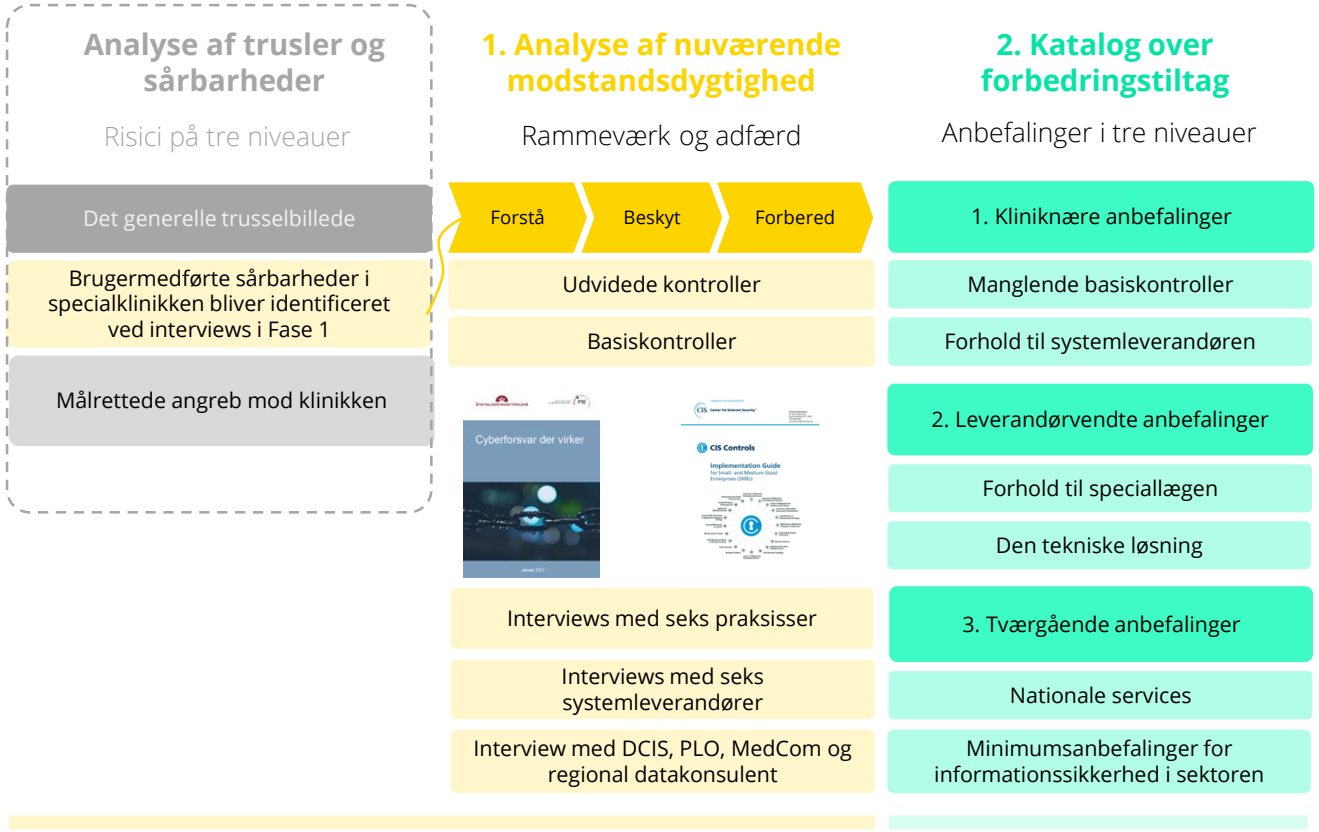
Typisk vil en informationssikkerhedsanalyse starte med trusler og risici (venstre del af figuren), men det kan ikke forventes, at den enkelte speciallæge foretager løbene risikovurderinger – eller generelt forholder sig aktivt til trusselsbilledet, hvorfor analysen i stedet har lagt eksisterende analyser og viden til grund og pragmatisk valgt at fokusere ressourcerne på det konkret handlingsanvisende. Der er således anlagt en kontrolbaseret tilgang, hvor der arbejdes kendte, prioriterede kontrolområder. Gennem kliniknære analyser og interviews udforskes prioriterede kontrolområder, som kan adressere observerede sårbarheder i klinikken.

Dette sker i **to trin**:

**1. Analyse af den nuværende modstandsdygtighed:** Afdækket gennem interviews med udvalgte speciallæger og hovedparten af systemhusene.

**2. Katalog over forbedringstiltag:** Opstilling af anbefalinger med baggrund i klinikanalysen samt interviews med leverandører og andre aktører.

PASSENDE IT-SIKKERHEDSNIVEAU FOR SPECIALLÆGER




Den mindre klinik er kendetegnet ved relativt få ansatte, et mindre budget til it-sikkerhed og begrænset viden inden for it. Derfor er det anbefalelsesværdigt for klinikken at fokusere på de tiltag, der giver den størst mulige dækning sammenholdt med indsatsen. Deloitte har anvendt anbefalingerne fra Digitaliseringsstyrelsen i *Cyberforsvar der virker* samt de kritiske kontroller (CIS top 20) med fokus på basiskontroller målrettet små og mellemstore virksomheder.

Der udvikles anbefalinger i alle tre lag vist ovenfor. De tværgående anbefalinger vil delvist kunne adressere forhold i de andre lag, og scope for disse bør derfor besluttes tidligt i udmøntningsprocessen.

# Hvad er informationssikkerhed?

Over de senere år er der i branchen for informationssikkerhed opstået konsensus om, hvordan beskyttelse af data eller information kategoriseres. De førende rammeværker og relevant lovgivning bruger denne samme kategorisering.

**VIGTIGT:** I diskussioner om informationssikkerhed i **sundhedsvæsnet** er det ofte aspektet fortrolighed, der fokuseres på. Men det er vigtigt, at man foretager en konkret afvejning af behovet for at tilgodese alle relevante aspekter af informationssikkerhed. Det er fx ikke hensigtsmæssigt at etablere et højt niveau af fortrolighed, hvis dette sker på bekostning af den nødvendige tilgængelighed til de informationer, der bruges for at udføre arbejdet i klinikken.

DIALOGEN OMKRING INFORMATIONSSIKKERHED AFHÆNGER AF HVILKE EGENSKABER, DER ER FOKUS PÅ AT BESKYTTE

| Egenskab | Beskrivelse | Eksempelfokus / dialog om |
|---|---|---|
| *Fortrolighed* | Information skal behandles ud fra den rette klassifikation. De fleste ved godt, at nogen information er mere fortrolig end anden. Dette er ikke mindst blevet væsentligt understreget med indførelsen af GDPR. | Kryptering, sikker mail, brugerawareness |
| *Integritet* | Information skal sikres imod at blive modificeret/ændret utilsigtet. Egenskaben handler om, sammen med fortrolighed, at give den tilstrækkelige og nødvendige adgang til information og beskytte imod uvedkommendes adgang. | Hashing, bruger-/ rettighedsstyring, antivirus |
| *Tilgængelighed* | Er information tilgængelig, når den behøves? Speciallægen er ofte afhængig af at kunne tilgå journaler under en konsultation, herunder at kunne tilgå systemer for at få adgang til medicinkort og øvrig relevant information om patienten. | Backup (RAID), beredskabsplaner, antimalware |
| *Autenticitet* | Kan man stole på data eller dem, man skriver med? Egenskaben er særligt i fokus, når der tales om eksempelvis digital signatur og kryptering, så det kan påvises, at en afsender af information er den, som vedkommende giver sig ud for at være. | Digital signatur |
| *Uafviselighed* | Egenskab ved information, der gør det muligt at bevise, at en given bruger har udført en given handling på et givet tidspunkt. Det handler for eksempel om logning eller lignende auditaktiviteter i systemer. | Logning og sporbarhed |

**Cyber- og informationssikkerhed i sundhedsvæsenet handler om *at*:**

beskytte patienternes data mod, at uvedkommende får adgang

sikre, at patienters information ikke utilsigtet bliver ændret eller går tabt

sikre, at patientsystemet er tilgængeligt ved behov, så journalpligten overholdes, og patientrisikoen minimeres

sikre, at ændringer, udstedelse af recepter mv. kan henføres til konkrete brugere

# Indsigt i de praktiserende speciallægers hverdag

Projektets fokuserer på at skabe indsigt i specialpraksislægernes faktiske hverdag. Projektet har fået unik adgang til at observere hverdagen i seks klinikker, hvor vi har kombineret cyberekspertise med etnografiske indsamlingsmetoder – og herved kortlagt lægernes og klinikpersonalets arbejde med informationssikkerhed. Vi har med samtykke fået lov til at deltage i 21 patientkonsultationer. Indsigter formidles blandt andet i form af visuelle brugerrejser.

En etnograf og en informationssikkerheds-specialist besøgte udvalgte klinikker i perioden **december 2019 til januar 2020**

Klinikkerne repræsenterede fem forskellige specialer og tre forskellige systemleverandører

Måling af modenhed inden for cyber- og informations-sikkerhed

**Fremgangsmåde**
(fysisk besøg i klinik)

**06** Interviews med praktiserende speciallæge

**09** Interviews med personale

**21** Observationer af patientkonsultationer

Observation af arbejdsgange

Optegning af konkrete arbejdsgange og kliniknære fokusområder

## Kliniknære tilstandsrapporter

Alle besøgte klinikker modtog en kliniknær rapport med observationer, anbefalinger og en samlet sikkerhedsscore af klinikken





# Analysemetode: kvalitativt feltarbejde

Det er afgørende via kvalitativt feltarbejde at opnå tilstrækkelig forståelse for arbejdssituationen hos speciallægerne, som der skal udvikles praksisnære forbedringstiltag til. Speciallægernes oplevelser står derfor centralt, og der er ligeledes fokus på betingelserne for at ændre adfærd.

**Kvalitativt feltarbejde**
Deloitte har anvendt en kvalitativ metode, da det ønskes at undersøge speciallægernes oplevelser og erfaringsprocesser. Den kvalitative tilgang er velegnet til undersøgelser, hvor formålet er at få indsigt i, hvordan noget gøres, siges, opleves, fremtræder eller udvikles. Det tilstræbes at forstå konkrete individer, hvor fokus er på at få indsigt i deres tanker, følelser og handlinger. Fokus er på at forstå subjektive perspektiver og herigennem betingelserne for at påvirke adfærd.

Metoden tager udgangspunkt i at kortlægge adfærd og behov ved at undersøge og forstå mennesker, processer, anvendelse af systemer og klinikkens fysiske rum. Hovedprincippet er at forstå menneskelig adfærd i den sammenhæng, hvori den forekommer naturligt, det vil sige i de naturlige omgivelser. Tilgangen indebærer derfor accept, tillid og dermed adgang til speciallægernes omgivelser igennem feltarbejde.

Deloitte foretog observationsstudier og semistrukturerede interviews, hvilket gav mulighed for at styre interviewene, samtidig med at speciallægerne frit kunne besvare spørgsmålene *(se spørgeramme i Bilag).*

***De fire linser i vores kvalitative feltarbejde***


**Brugerrejser**
Til dokumentation af det kvalitative feltarbejde udarbejdes overordnede brugerrejser. En brugerrejse kortlægger hvilke sekvenser, en speciallæge gennemgår. En brugerrejsekortlægning giver et overblik over de faktorer, der påvirker brugeroplevelsen ud fra speciallægens perspektiv. Ved at basere kortlægningen på disse brugerindsigter skabes et overblik over kontaktpunkter mellem speciallægen, praksissystemer og andre aktører. Kontaktpunkterne danner omdrejningspunktet for identifikation af problemområder og forbedringsmuligheder.

Alle stadier af analysen gennemlyses af et cyber- og informationssikkerhedsfokus: Hvordan sikres de data, der overdrages fra patient til læge? Hvem har adgang til hvad hvornår? Hvilke systemer anvendes, og hvordan er disse konfigureret? Hvilke overvejelser er foretaget om de fysiske rum?

**Primære aktører**
For at forstå oplevelser og forventninger er det vigtigt at stille skarpt på de primære brugeres behov og udfordringer, da deres arbejdsgange har forskellige fokus og problematikker. De primære aktører er følgende:

**1) Speciallægen**

**2) Speciallægens personale**

**3) Systemleverandøren**

**Følgende typer kliniktyper er besøgt**

1) Klinikker der ifm. diagnosticering anvender udstyr

2) Klinikker der udelukkende anvender samtalebaserede konsultationer

3) Énmands-klinikker samt større klinikker med mere personale eller deleklinikker.

4) Klinikker med såvel korte som længere patientforløb

# Udvælgelse af leverandører

Da systemunderstøttelsen og leverandørens processer i væsentlig grad betinger arbejdsgangene i den enkelte praksis, vurderes observationer vedrørende leverandørerne som udgangspunkt at være relevante på tværs af deres kunder.

Analysen er baseret på en kombination af leverandørinterviews og klinikbesøg. På leverandørsiden er der lagt vægt på at interviewe alle leverandører med en væsentlig markedsandel. Da systemunderstøttelsen og leverandørens processer i væsentlig grad betinger arbejdsgangene i den enkelte praksis, vurderes observationer vedrørende leverandørerne som udgangspunkt at være relevante på tværs af deres kunder. Dette bestyrkes af, at der er konstateret begrænset variation på tværs af forskellige klinikker med samme leverandør (med forbehold for stikprøvens størrelse). Med argumentet om, at leverandørerne er det vigtigste parameter, kan der således alt andet lige tales om fire niveauer af dækning og gyldighed (som vist til højre).

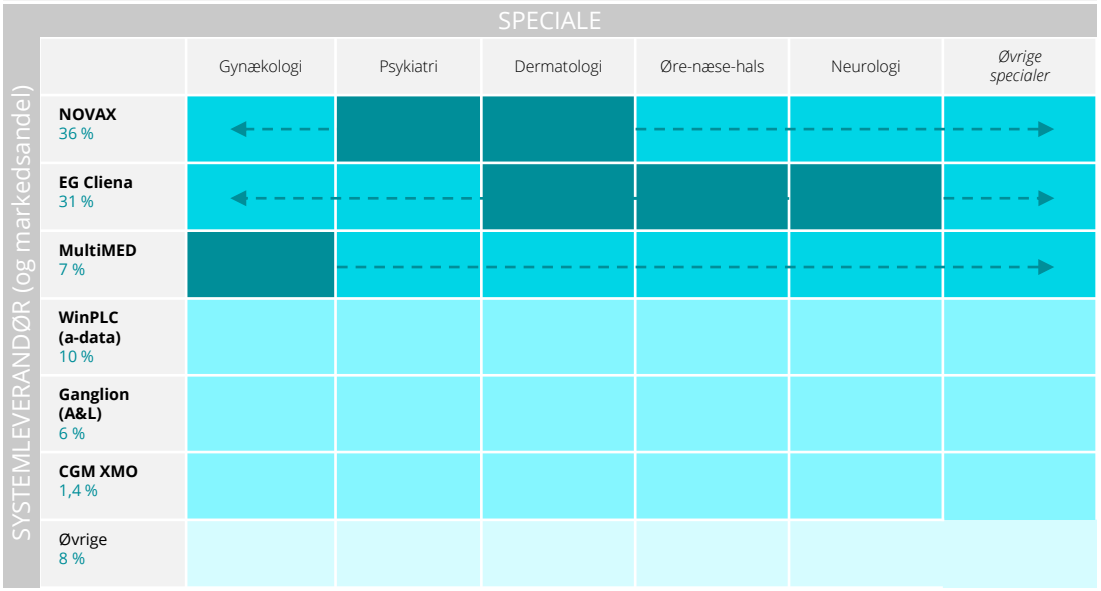
På kliniksiden er udvælgelsen sket ud fra en kombination af leverandør og speciale, hvor der er tilstræbt den mest sigende spredning på tværs af specialer. Praktisk tilgængelighed har dog også været en faktor. Således er der eksempelvis ikke interviewet en anæstesilæge*. Grundet den måde, udvælgelsen af klinikker konkret har fundet sted på, er der endvidere en overrepræsentation af klinikker med en højere end gennemsnitlig interesse i informationssikkerhed. I det omfang analysen konstaterer, at klinikkerne har udfordringer med at gennemføre de påkrævede tiltag i det daglige arbejde, må disse konklusioner alt andet lige forventes at være skærpede, hvad angår den bredere population.

*) Anæstesilægen skiller sig ud: Anæstesilægen har ikke egen klinik, men leverer en service til en anden klinik. Der findes to varianter: Enten bruger anæstesilægen klinikkens systemer, eller også bruger lægen systemer på egen medbragte pc. I begge tilfælde er der rent sikkerhedsmæssigt særlige opmærksomhedspunkter. Analysen har dog ikke omfattet klinikbesøg hos/med anæstesilæger, så der bør i det videre arbejde med at udmønte anbefalingerne være en opmærksomhed på også at favne disse varianter og deres særlige behov samt risici.

NIVEAUER AF DÆKNING OG DERMED GYLDIGHED

| Niveau 1. Lav | Niveau 2. Middellav | Niveau 3.Middelhøj | Niveau 4. Høj |
|---|---|---|---|
| Baseres på analysens generelle indsigter, herunder for specialer, som ikke er særskilt afdækket | Leverandør interviewet, men ingen klinikbesøg<br>✓ Systemleverandør-interview | Leverandørinterviews og indirekte klinikbesøg<br>✓ Systemleverandør-interview<br>✓ Besøg ved andet speciale med samme journalsystem | Både specialet og leverandøren er direkte dækket<br>✓ Systemleverandør-interview<br>✓ Besøg i klinik med systemet |

**ANALYSENS DÆKNING OG GYLDIGHED**



# Et passende rammeværk for informationssikkerhed

Få konkrete initiativer adresserer op imod 80 procent af alle cyberangreb.

**En konkret prioriteret plan for cybersikkerhed**

Flere standardudstedende organisationer har udarbejdet bedste praksis-beskrivelser af cybersikkerhed, såkaldte security frameworks (eksempelvis ISO 2700X og NIST 800-serien). Disse rammeværker beskriver, hvordan organisationer kan arbejde med informations-sikkerhed, herunder roller og ansvar, udarbejdelse af politikker og procedurer samt beskrivelse af konkrete sikkerhedstiltag.

Det kan være udfordrende for mindre organisationer at følge disse rammeværker; ofte råder den lille organisation ikke over egne specialister inden for cyber- og informationssikkerhed og har heller ikke et tilsvarende it-budget. For speciallægeklinikken er dette i høj grad tilfældet. For at adressere denne problemstilling har blandt andet CIS (Center for Internet Security, USA) og danske myndigheder udviklet mindre vejledninger, som arbejder prioriteret med informationssikkerhed ud fra den lille organisations hverdag, med afsæt i spørgsmål som:

- Hvor skal man starte?
- Hvornår er nok nok?
- Hvordan foretages afvejningen af på den ene side at have et effektivt, tilstrækkeligt cyber forsvar og på den anden side at passe sin klinik?

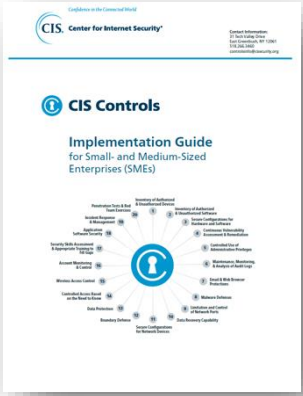
Deloitte har derfor valgt at basere metodegrundlaget med inspiration på det vejledende rammeværke fra CIS – i en SMV-version (de såkaldte kritiske kontroller) – og vejledningen fra som Center for Cybersikkerhed. Fordelen ved denne tilgang er, at den har en særlig praktisk karakter med fokus på følgende:

- Hvordan man for færrest mulige midler får den største grad af forsvar: Hvad virker?
- I hvilken prioriteret rækkefølge initiativerne bør planlægges?

ANBEFALINGER SOM KLINIKKERNE HOLDES OP IMOD


Center for Cybersikkerhed har udarbejdet gode råd om cyberforsvar. Anbefalingerne består af syv trin:

- Trin 1-4: grundlæggende sikringstiltag
- Trin 5-7: udvidede sikringstiltag




CIS har udarbejdet en anerkendt liste over 20 kritiske kontroller: de såkaldte top 20.

Ved at arbejde med top 20 inden for SMV-segmentet, herunder speciallægepraksisser, sikres en praktisk tilgang til informationssikkerhed.

# SIKKERHEDSBAROMETRET

Observationer i klinikken blev analyseret og fik tildelt en score ud fra sikkerhedsbarometrets tre niveauer. Speciallægerne fik her en indikation på, om klinikkens sikkerhedsniveau lå i rødt, gult eller grønt område.


**Kendetegn for modenhedsniveauerne**
selv en lille indsats kan gøre en stor forskel

Den observerede modenhed for de respektive klinikker fordeler sig på disse niveauer

**Formaliseret/prioriteret**

- Arbejdet med it-sikkerhed er indarbejdet i budgettet; der er fx sat penge af til awarenesstræning og serviceaftaler i tilfælde af nedbrud.
- Klinikken har nedskrevne procedurer og fremmer aktivt awareness, eksempelvis ved kaffemaskinen, toilettet og andre steder i klinikken.
- Der er løbende dialog med systemleverandøren om it-sikkerheden i tilkøbte systemer.
- Klinikken er opmærksom på, hvilke tiltag der virker; der skelnes mellem basiskontroller (robusthed) og nice to have. Klinikken arbejder prioriteret med tiltagene.

**Ad hoc**

- Der er ikke sat penge af til it-sikkerhed i budgettet.
- Arbejdet med it-sikkerhed er præget af tilfældige tiltag, for eksempel passwordsikkerhed.
- Procedurer er ikke skrevet ned, eller de følges ikke.
- Der er ingen dialog med systemleverandøren i forhold til it-sikkerheden.
- Der er ikke oparbejdet viden om prioritering af tiltag, dvs. hvad der gør en forskel.
- Klinikken viser interesse for informationssikkerhed, men har svært ved at prioritere tiltag på grund af manglende indsigt.

**Ikke i fokus**

- Der er ikke sat penge af til it-sikkerhed i budgettet.
- I værste fald er it-sikkerhed ikke en prioritering; der er en opfattelse af, at det enten er sikkert og bøvlet eller mindre sikkert, men funktionelt, hvilket kan medføre en uheldig kultur.
- Arbejdet med it-sikkerhed er (næsten) ikke-eksisterende.
- Procedurer findes ikke og er ikke på tegnebrættet.
- Der er ingen dialog med systemleverandøren i forhold til it-sikkerheden.
- Systemsikkerhedspakken er fravalgt for at spare penge.
- Der er ikke oparbejdet viden om prioritering af tiltag, dvs. hvad der gør en forskel.

*"Jeg oplever ikke, at speciallægen efterspørger it-sikkerhed. Når vi åbner dialogen omkring sikkerhed, opleves det oftest som et forsøg på mersalg. Det er ærgerligt."*
*Systemleverandør*


# 4. De seks system-leverandører

I dette afsnit præsenteres indsigter fra interview med de seks udvalgte systemleverandører, der tilsammen dækker 92 % af markedet. Der henvises endvidere til ledelsesresumeet.

# Opsummering vedr. lægesystemleverandørerne

Markedet for journalsystemer er domineret af få spillere, hvor de omfattede seks leverandører udgør 92 % af markedet.

Informationssikkerhed og tilknyttet vejledning ses ofte inkluderet i den hostede løsning, men er tilkøb, hvis der vælges en on-premise-løsning. Leverandørerne tilkendegiver, at tilkøb af informationssikkerhed oftest fravælges af speciallægen, da dialogen opleves som mersalg.

Alle leverandører tilbyder ydelser relateret til it-sikkerheds som tilkøb; dog er det kun enkelte leverandører, der arbejder systematisk med cyber- og informations-sikkerhed. Ud af de seks system-leverandører er kun to blevet certificeret efter it-sikkerhedsstandarden ISO27001.

En ændret prioritering af tiltag vedr. informationssikkerhed hos system-leverandøren, også som opfølgning på Ezenta-rapportens findings, vurderes at kunne skabe et bedre fundament for sikker it-udvikling og ultimativt et mere sikkert produkt til glæde for såvel praksisserne som hele sektoren.

| | *Forhold* | MultiMED | XMO | Ganglion (Aver & Lauritzen) | WIN PLC (a-data) | EG Clinea | Novax |
|---|---|---|---|---|---|---|---|
| **Størrelse i markedet for speciallæger** | Antal speciallægekunder som andel af total antal speciallæger (943) | 69 (7%) | 13 (1,4%) | 56 (6%) | 98 (10%) | 294 (31%) | 340 (36%) |
| **Sikkerhedsrådgivning** | Tilbyder generel sikkerhedsrådgivning og anbefalinger | X | X | X | X | X | X |
| | Tilbyder målrettet it-sikkerhedsscreening og rådgivning af klinik som en service | X | | X | X | | |
| **Infrastruktur løsninger til understøttelse af Patienthåndteringsprogram eller klinikken generelt** | Tilbyder at være it-service provider | X | X | X | X | X | |
| | Tilbyder hostet løsning | X | (X) | X | X | X | X** |
| | Tilbyder levering og installering af on-premise-løsning | X | X | X | X | X | X |
| **Sikkerhedsløsninger som tilkøb*** | Tilbyder backup som tilkøb | X | X | X | X | X | X |
| | Tilbyder antivirus og patch management som tilkøb | X | X | X | X | X | X |
| | Tilbyder firewallkonfiguration som tilkøb | X | X | X | X | X | X |
| | Tilbyder brugerstyring (hovedsageligt tilkøb) | X | X | X | X | X | X |
| **Leverandørens interne arbejde med anderkendte rammeværk for it-sikkerhed** | ISO 27001-certificeret (interne processer lever op til bedste praksis indenfor informationssikkerhed) | X | | | X | | X |
| | Inspireret af ISO 27001/andet bedste praksis-rammeværk | X | | X | X | X | |

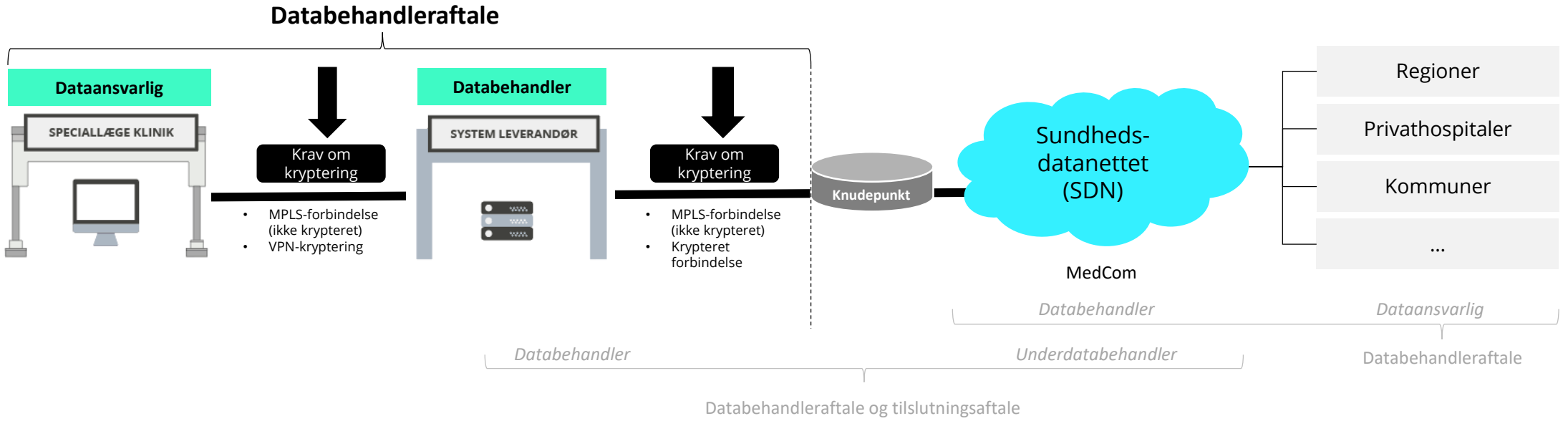
*) Når man vælger den hostede løsning, vil alle listede sikkerhedsforanstaltninger være inkluderet uden mulighed for fravalg.

**) Den hostede løsning kan dog ikke tilbydes alle specialer, da ikke alle kan levere data til Novax' hostede øsning (afhænger af apparaturintegration).

# Systemleverandøren og speciallægen bør indgå dialog omkring sikker transport af data

Det er en udbredt fejlopfattelse, at data beskyttes gennem kryptering på Sundhedsdatanettet (SDN). Den enkelte leverandører skal imidlertid selv sikre den fornødne kryptering. Praksissektorens standarddatabehandleraftaler med systemhusene bør således have indskrevet krav om kryptering af data op indtil overdragelse af data på SDN-knudepunktet.




**Behov for at afklare databehandleraftalekrav og samspillet i økosystemet, så der både er høj teknisk sikkerhed (kryptering mv.) og juridisk compliance (GDPR mv.):**
Undervejs i analysen er det fremkommet, at der på den tekniske side er en fejlopfattelse af, at data automatisk er krypteret på Sundhedsdatanettet (SDN). Endvidere er der tilsvarende på den juridiske side udtrykt uklarhed angående hvilke databehandleraftaler, den enkelte aktør i netværket er ansvarlig for. Aftalekrav og ikke mindst ansvar for beskyttelse bør være entydigt og ensartet på tværs af værdikæden, herunder i form af fælles krav til hvordan, data transporteres. En afklaring bør koordineres med sektorstrategiens initiativ 2.5 om skærpede sikkerhedskrav til it-leverandører, som også omfatter en analyse af muligheden for leverandørstyring gennem SDN.

Det anbefales følgelig, at praksissektorens standarddatabehandleraftaler med systemhusene får indskrevet et krav om kryptering.

Fremstillingen er baseret på gengivelse fra følgende (uden særskilt juridisk analyse af Deloitte):
- https://www.medcom.dk/systemforvaltning/sundhedsdatanet-sdn/infrastruktur
- https://www.laeger.dk/databeskyttelse

*"Vi mangler en sikker mail. Jeg har forsøgt at få det. Man ryster nærmest på hænderne, når man sender et fysisk brev i stedet – man ved jo ikke hvor, det ender."*
*Praktiserende speciallæge*

# 5. Elementer i en implementering

I dette afsnit præsenteres forslag til næste skridt, rammevilkår og mulighedsrum samt en værktøjskasse for bedre informationssikkerhed.

# Næste skridt

Overvejelser om proces og forankring.

**Den videre proces skal aftales parterne imellem og under iagttagelse af andre igangværende initiativer, herunder sektorstrategien og anbefalede minimumskrav.**

Anbefalingerne er derudover gensidigt afhængige, særligt på to måder:

1) Anbefalede minimumskrav vil alt efter form og detaljeringsgrad adressere en delmængde af de klinik- og leverandørnære anbefalinger.
2) Hvis parterne beslutter, at der bør ydes en større service til de enkelte læger, vil dette konkret kunne komme til udtryk ved, at lægerne får bistand til en del af de kliniknære anbefalinger.

Overordnet anbefales således følgende proces og forankring:

1. Parterne (SUM, SDS/DCIS, FAPS og PLO) aftaler i fællesskab tilgang til og forankring af de tværgående forhold, herunder også konkret hvorvidt klinik- og leverandørnære anbefalinger helt eller delvist forventes afløftet på tværs. Dette vil definere rammerne for de øvrige anbefalinger. Vi anbefaler her, at der gennemføres et fælles *cyber lab* mht. at opnå konsensus om anbefalinger, plan og tilgang (som vist nedenfor).
2. De klinik- og leverandørvendte anbefalinger tilpasses om nødvendigt pba. ovenstående aftaler.
3. Den kliniknære del kan herefter formidles af FAPS, ledsaget af de to ark med værktøjskassen og praksisnære råd og vejledninger. Det vil i denne sammenhæng være centralt, at det samtidig tydeligt kommunikeres hvor og hos hvem, der kan søges supplerende rådgivning.
4. Den leverandørvendte del kan drøftes med leverandørerne organiseret i det fælles PL-forum. Processen bør her afstemmes med PLO. Endvidere skal de leverandører, som ikke er organiseret i PL-forum, kontaktes særskilt.

Da anbefalingerne kan være udgiftsdrivende, bør dette hensyn indgå i beslutningen om proces. Ifølge det oplyste vil det igangværende arbejde med minimumskrav forventeligt blive formuleret som anbefalinger og ikke krav – hvorved det vil være overladt til markedsmekanismen og dialogen parterne imellem at sikre, at anbefalingerne i relevant omfang følges.

Individuelt tilpassede anbefalinger til de deltagende praksisser er allerede fremsendt som led i arbejdet med at færdiggøre analysen.

**1**

**Konsensus om anbefalinger**

**2**

**Plan og forankring**

**3**

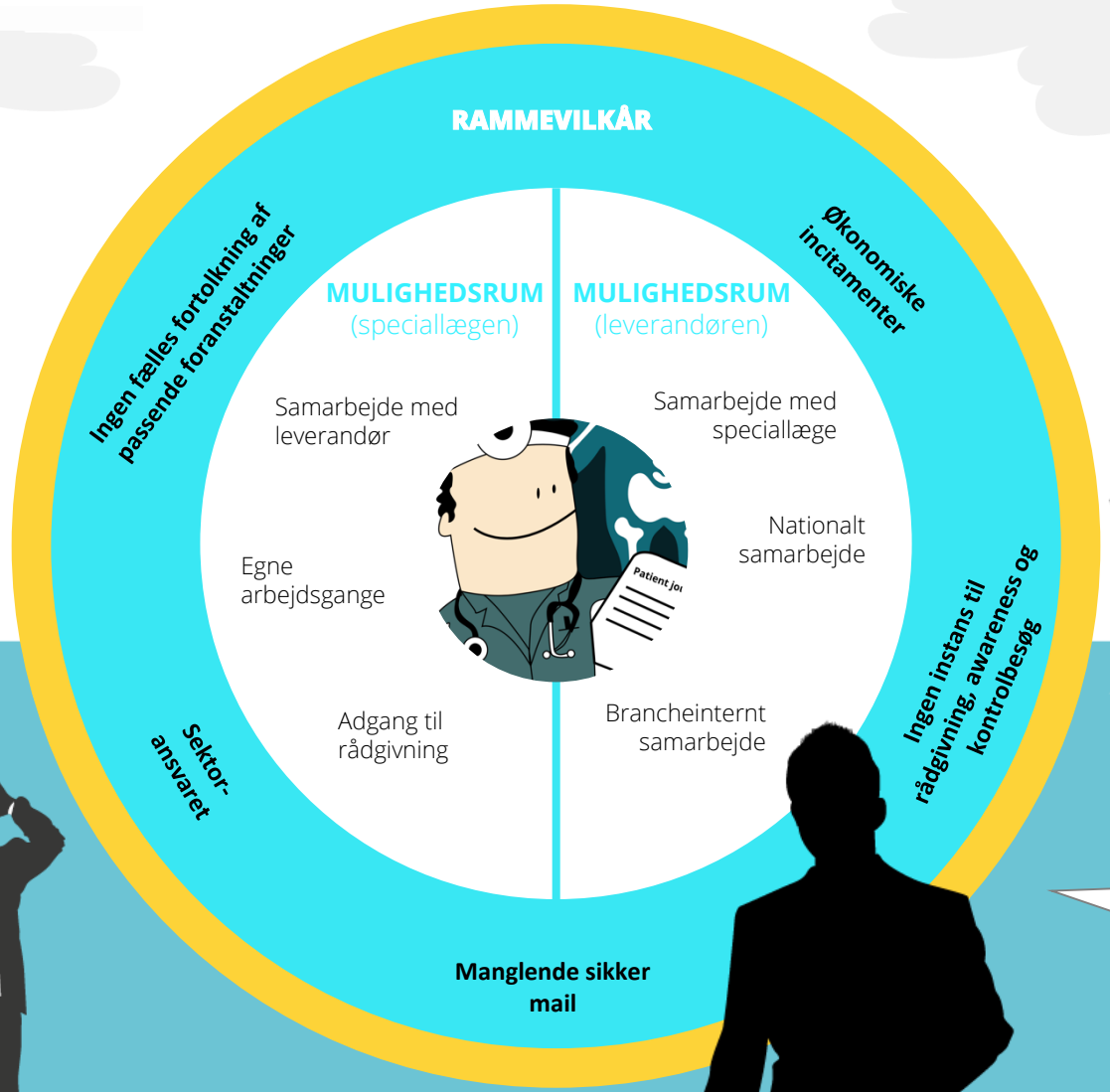
**Implementering**

# Rammevilkår og mulighedsrum

Nogle af de identificerede sårbarheder har speciallægerne selv umiddelbart mulighed for at påvirke, hvilket peger ind i det ene sæt af anbefalinger, nemlig de **praksisnære anbefalinger**. Tilsvarende er der et sæt af **anbefalinger til leverandørerne**. Endelig er der som et tredje ben **tværgående anbefalinger om at ændre rammevilkårene**.

Analysen har vist, at der på det strukturelle niveau er en række **rammevilkår,** som i afgørende grad betinger klinikkernes muligheder for selv at løfte informations-sikkerheden yderligere. Her er der en potentiel spænding mellem sektoransvars-princippets insisteren på, at ansvaret i sidste ende er den enkelte læges, og på den anden side det praktiske behov for, at en tværgående instans i højere grad hjælper lægerne med at løfte ansvaret.




"Det er for teknisk; derfor betaler jeg mig fra det, og så må jeg håbe, at min leverandør har styr på det."
*Praktiserende speciallæge*

"Det ville give os stor værdi, hvis vi kunne få nogle tekniske minimumskrav eller nogle anbefalinger til hvordan, vi bedst når ud til speciallægerne."
*Sektormyndigheden DCIS*

"Forventningsafstemning er for ringe, og den fylder for lidt. Nogle læger tror, at leverandører har ansvaret."
*Systemleverandør*

# Anbefalinger fører ikke i sig selv til adfærdsændring

Det er vigtigt, at speciallægen støttes til at vedligeholde en adfærdsændring i hverdagen. Derfor bør forandringsprocessen designes, så der er adgang til rådgivere i eller omkring klinikken for at bibeholde speciallægens fokus på informationssikkerhed.

**Adfærd = motivation + evnen til handling + trigger/feedback**

En speciallæge er uddannet i patientsikkerhed, hvorfor triggers omkring hygiejne ligger speciallægernes faglighed nært. Herudover findes flere hjemmesider, som pointerer utilsigtede hændelser i forbindelse med patientsikkerhed. Her kan lægerne lære af og forstå eventuelle fejl. Jo flere triggers, der findes eller skabes til en handling, jo større chance er der for en adfærdsændring.

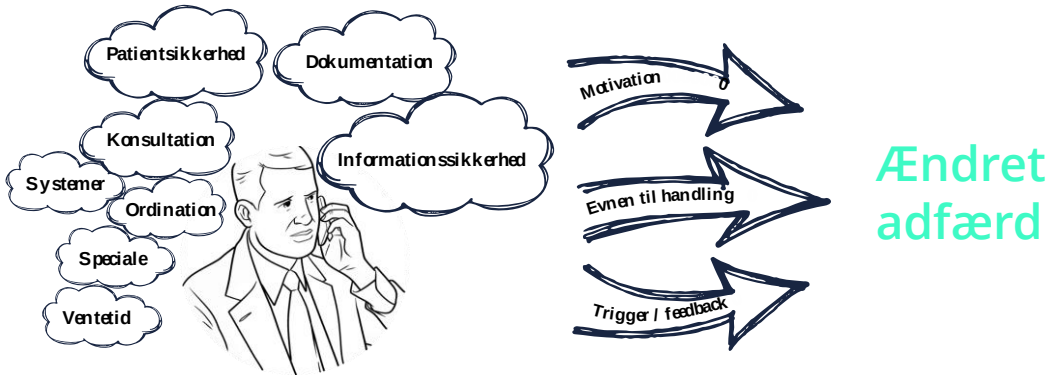
Informationssikkerhed ligger modsat patientsikkerhed længere fra speciallægernes faglighed. Speciallægerne ønsker høj informationssikkerhed *(motivation),* men:

**1) De kender ikke til tekniske handlemuligheder for at højne informationssikkerheden *(evne).***
**2) De ved ikke, hvilke standarder de skal gå efter *(trigger).***
**3) Der er usikkerhed om, hvem de skal spørge til råds *(trigger).***
**4) De modtager ingen feedback på eventuelle handlinger *(feedback).***

Ud fra ovenstående kan man argumentere for, at kun et element i adfærdsændrings-ligningen er til stede (motivationen). Først når alle elementer er til stede, vil en adfærdsændring ske og over tid kunne danne ændrede vaner. Herudover kan man argumentere for, at en adfærdsændring hos specialiserede og travle fagpersoner kræver yderligere, da tilpasningstiden til nye mønstre er sparsom.

I adfærdsdesign taler man om et ubevidst mønster i hjernen ved navn *tilgængelighedsheuristik.*[2] Mennesker bruger denne til at vurdere sandsynligheden for, at noget sker. Vurderingen bygger på den information, vi har i forvejen. Dette betyder, at når speciallægen ikke ofte bliver præsenteret for utilsigtede hændelser i forbindelse med informationssikkerhed i egen branche, vurderes sandsynligheden for et cyberangreb som lav, hvilket gør prioriteringen af informationssikkerhed mindre vigtig. En af de besøgte

Klinikker havde oplevet et cyberangreb på klinikkens it-udstyr. Denne klinik var samtidig den eneste ud af de besøgte klinikker, som havde udarbejdet en beredskabsplan og havde nedskrevne procedurer vedrørende informationssikkerhed, da de oplevede sandsynligheden for angreb som større end de andre klinikker. For at udføre en adfærdsændring i forbindelse med informations-sikkerhed skal speciallægerne oftere informeres om utilsigtede hændelser.




Aftaler kan medvirke til at fremme en handling, da der herved er skabt en konkret anledning. Således kunne en tredjepart for eksempel udføre et followup i klinikken og på den måde give speciallægen en feedback samt give mulighed for besvarelse af eventuelle kliniknære spørgsmål. Dette kunne både være en ekstern datakonsulent eller en (system)leverandør, som man tilkøbte denne service hos.

*1. The Fogg Behavior Model (FBM)*
*2. Tilgængelighedsheuristik: Kilde: Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. Cognitive psychology, 5(2), 207-232.*

# Værktøjskasse for god it-sikkerhed

Som supplement til de kliniknære anbefalinger er der her vist en mere generel værktøjskasse inden for god it-sikkerhed. Der er fokus på de tekniske forhold, som i mindre organisationer bør adresseres for at have en tilstrækkelig høj sikkerhed. Forholdene kræver en vis teknisk indsigt i informationssikkerhed, hvorfor det for mange klinikker vil være noget, der skal adresseres i samarbejde med en rådgiver og/eller systemleverandør.

| | Forstå situationen | Beskyt kritisk information | Reager på brud – og vend tilbage til stabil drift |
|---|---|---|---|
| Formål | Klinikken skal være bevidst om, hvilken kritisk information der håndteres, samt hvor informationen bliver anvendt og lagret. Det er vigtigt at være i kontrol. Derfor er en del af forståelsen at vide, hvilke tekniske enheder der er koblet op på klinikkens netværk, herunder hvordan disse enheder kan være sårbare, og hvordan de beskyttes. | Malware udnytter enten sårbarheder, der opstår som følge af usikker konfiguration af udstyr, eller sårbare programmer.<br>For at beskytte mod angreb er det vigtigt, at medarbejderne har styr på god sikkerhedshygiejne gennem løbende awareness, samt at processer og teknisk udstyr er gearet til it-sikkerhed. | Det er ikke længere et spørgsmål om, hvorvidt virksomheder rammes af cyberangreb, men hvornår og hvordan man tackler et angreb. Det er et stressende forløb, hvor der opstår en masse spørgsmål. Her er det vigtigt med en køreplan: Hvor skal man ringe hen, hvordan kommer vi tilbage på sporet, hvad siger vi til vores kunder, skal vi indrapportere brud på persondatasikkerheden? |
| Grundlæggende sikringstiltag/basiskontroller | ✓ Tilsikr, at de rette tekniske kompetencer er til rådighed ved behov (for eksempel serviceaftale)<br>✓ Vedligehold en liste over hardware og kritisk data (computere, servere, bærbare, printere, telefoner mv.)<br>✓ Vedligehold en liste over software<br>✓ Krypter trådløse netværk (WPA2)<br>✓ Minimer brugen af administratorbrugere (domæne- eller lokaladministratorrettigheder, særligt i forhold til privat/arbejdsmæssig brug)<br>✓ Udarbejd en passwordvejledning (minimumlængde, kompleksitet, forældelse og genbrug)<br>✓ Vedligehold en positivliste over godkendte programmer (der findes ikke software til at sikre, at der ikke installeres øvrig software). | ✓ Skab awareness om cybersikkerhed<br>✓ Opdater styresystem og programmer (særligt browsere og plugins)<br>✓ Brug en firewall, både i routeren og på computeren<br>✓ Minimer brugen af bærbare medier (for eksempel usb-stik, cd'er og bærbare harddiske)<br>✓ Brug et antivirusprogram og tjek at automatisk opdatering er slået til<br>✓ For adgang til kritisk information anbefales det at bruge to-faktor-autorisation (fx brugernavn/password + kode fra dongle/telefon)<br>✓ Ændr standardpasswords på udstyr<br>✓ Krypter enheder med kritisk information<br>✓ Scan klinikkens netværk periodevis for at identificere sårbarheder (der findes gratis programmer, men overvej professionel vejledning)<br>✓ Efterprøv personalets viden omkring phishing (mailangreb) og vishing (telefonangreb)<br>✓ Implementer tvungen skærmlås, hvis brugeren er inaktiv<br>✓ Påsæt privacy-filter på computere og andre enheder, hvor der er risiko for, at patienter eller øvrige personer kan se "over skulderen". | ✓ Tilsikr, at der foretages backup (automatiske muligheder foreligger)<br>✓ Foretag løbende test af restore (genetablering)<br>✓ Tilsikr, at mindst en backup ikke kan tilgås fra netværket (så de(n) ikke kan tilgås i forbindelse med et angreb)<br>✓ Lav en oversigt over personer, som skal underrettes i tilfælde af angreb (enten eget personale og/eller en leverandør, som leverer "incident management")<br>✓ Roller og ansvar beskrives kort og præcist<br>✓ Telefonnummer<br>✓ Vedligehold en liste over relevante organisationer, juridisk bistand, offentlige institutioner<br>✓ Skabeloner til underretning. |
| Inspiration til speciallægen | • Vejledning i passwordsikkerhed: https://fe-ddis.dk/cfcs/publikationer/Documents/Vejledning-Passwordsikkerhed.pdf<br>• Vejledning i informationssikkerhed: https://sikkerdigital.dk/media/10148/informationssikkerhedspolitik-lille-model.pdf<br>• Vejledning i databeskyttelse: https://www.laeger.dk/databeskyttelse | • Sikker Digital om gode digitale vaner: https://sikkerdigital.dk/virksomhed/fem-gode-raad-der-styrker-din-virksomheds-it-sikkerhed/faa-gode-digitale-vaner/<br>• Kør for eksempel MS Baseline Security Analyzer for at se, hvilke opdateringer der mangler, eller om der anbefales konfigurering. | • Vejledning i informationssikkerhed i leverandørforhold: https://sikkerdigital.dk/media/11165/vejledning-informationssikkerhed-i-leverandoerforhold.pdf<br>• Vejledning i hændelseshåndtering: https://sikkerdigital.dk/myndighed/haendelseshaandtering/<br>• Vejledning i brud på persondatasikkerhed: https://www.datatilsynet.dk/media/6558/haandtering-af-brud-paa-persondatasikkerheden.pdf<br>• Indberetning af brud på sikkerhed: https://indberet.virk.dk/myndigheder/stat/ERST/Indberetning_af_brud_paa_sikkerhed |

Forslag

# God it-hygiejne: Hvad kan jeg gøre i min praksis?

**Kernetiltag**: Forslag til hvordan de ni kliniknære anbefalinger på side 20 kan uddybes og gøres endnu mere konkrete for speciallægeklinikkerne. Forslagene vil kunne omsættes til en grafisk overskuelig plakat som vist på side 46. Hensigten er, at speciallægerne bliver guidet til at stille sig selv og deres systemleverandør de rigtige spørgsmål.

### Sørg for klare aftaler om ansvar og arbejdsdeling med systemleverandøren

- Gennemgå leverandørkontrakten og bed leverandøren om at uddybe eventuelle uklare forhold.
- Sørg for at I er enige om hvordan arbejdsdelingen omkring informationssikkerhed i praksis skal forstås.
- 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.

### 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.

### Opsæt informationsmateriale og træn awareness

- Oplys om god it-hygiejne i klinikken og brug visuelle virkemidler samt evt. nudging-teknikker til at sikre, at informationssikkerhed bliver en naturlig del af hverdagen (kan være en plakat ved kaffemaskinen eller en vejledning under skrivebordsmåtten – se også vejledninger mv. på side 41 ovenfor).
- Planlæg at vi periodisk (mindst årlig) træner informationssikkerhed – kan både være fysiske øvelser med en ekstern ekspert eller online awareness-kurser.
- Tænk god it-hygiejne og god brugeradfærd ind i jeres intro-forløb for nye medarbejdere.

### 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. Konfigurér computeren med en gruppepolitik, som tilsikrer, at programmer ikke automatisk kan startes fra en usb-stick.
- 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 (så vidt muligt; baseres på en konkret vurdering).
- 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.

### Tag stilling til håndtering af nødsituationer og til brugernes adgange

- Planlæg og aftal hvad I 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).

### Tjek klinikkens backupaftale

- Tages der kun backup af lægesystemet? Eller også af fællesdrev?
- Hvor ofte tages der backup? Vurdér om det er tilstrækkeligt.
- Er det entydigt, der har ansvar for at sikre og teste, at backuppen fungerer og at data reelt kan reetableres?
- Er det entydigt hvem, der har ansvar for at tage backup – og for at reagere, hvis backuppen fejler?
- Normalt tages der ikke backup af pc'ernes skriveborde, så undgå at lægge data der.

### 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).

### 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.
- Sårbarhedstesten skal bl.a. omfatte følgende kontroller:
- Kontrollér at proces for brugeradministration overholdes, og at klinikken foretager brugerreview/oprydning.
- Kontrollér opdatering/patching af systemer, firewall, antivirus, 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.

### 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). – *Patienter forventer en høj grad af fortrolighed i behandling af forespørgsler og udveksling af information.*

*”Vi kan altid ringe til vores system-leverandørs hotline eller direkte til deres teknikere i særlige tilfælde.”*
*Praktiserende speciallæge*

*”Gid jeg havde en der kunne rådgive mig. En der snakker dansk og ikke ‘it’, og som i hyppige intervaller gennemtjekker det hele.”*
*Praktiserende speciallæge*

# 6. Perspektiver

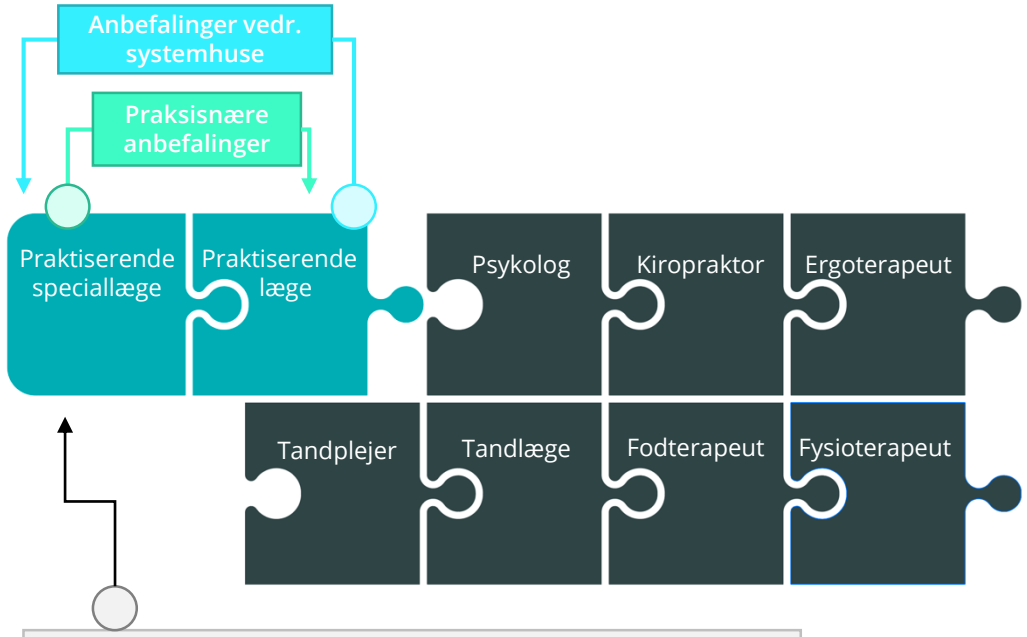
# Perspektiver (1/2)

Bidrag til den fortsatte vidensopbygning i sektoren: Indholdsmæssigt er analysen er et yderligere bidrag til et sammenhængende og risikobaseret overblik over sundhedsvæsenets mindre, selvstændige erhvervsdrivende aktører, der foruden praksissektoren også omfatter en række andre behandlere.

**Bidrag til den fortsatte vidensopbygning i sektoren**

Analysen har bygget videre på tidligere foretagne analyser, særligt Analyse af praksissektorens systemhuse (2017. Nærværende analyse har suppleret det hidtidige leverandør- og teknikfokuserede arbejde med et mere kliniknært og brugerfokuseret perspektiv. Da leverandørerne i vid udstrækning er de samme på tværs af praksissektoren, vurderes nærværende analyses leverandørrettede konklusioner som udgangspunkt at kunne overføres til almen praksis (der dog kan have anderledes opsætninger), ligesom 2017-18-analysen af leverandørsikkerheden omvendt også forventes at gælde for leverandørernes services til speciallæger.

I et bredere perspektiv er de største og mest databærende aktører i feltet af mindre private behandlere nu belyst. De kliniknære og adfærdsmæssige indsigter forventes til en vis grad at kunne overføres til øvrige behandlere, om end ikke uden supplerende analyse. En sådan analyse bør særligt fokusere på systemunderstøttelse/leverandører, data, typen af patientforløb, graden af formalisering af krav og hvilken rådgivning mv. der tilbydes fra branceorganisationer mv.



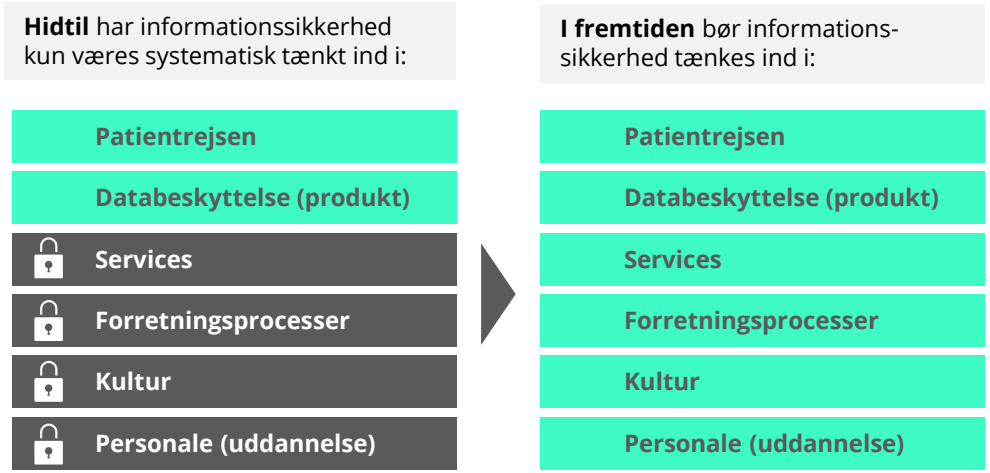
# Perspektiver (2/2)

Bidrag til en mere brugercentreret tilgang: Metodisk kan analysen ses som et bidrag til en syntese af informationssikkerhedsfaglig og etnografisk metode.

**Bidrag til en mere brugercentreret tilgang**

Databeskyttelse handler om mere end bare at implementere et sikkert system. Det handler om hvordan, databeskyttelse end-to-end bliver tænkt ind i en virksomheds eller organisations produkter, services, kultur og forretnings-processer. Udtrykket "Privacy by Service Design" henfører til databeskyttelse gennem teknologidesign. PbSD tager udgangspunkt i brugeren, som er omdrejningspunktet i løsningen.

PbSD er under udvikling som en tilgang, der sikrer, at speciallægen/leverandøren indarbejder databeskyttelse som en integreret del af virksomhedens forretningsprocesser, værdikæde og produktlivscyklus. Sammenkoblingen af henholdsvis 1) privacy by design og 2) service design sikrer på den måde, at der designes til brugerens kontekst og tilpasset nuværende forretningsprocesser. Det forventes, at privacy herved lettere vil kunne blive integreret i arbejdsgange og således i mindre grad vil opleves som en ny, tidskrævende ekstraopgave.



# Appendiks: Leverandør-oversigt

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.*
  - *Kontrollér wi-fi-indstillinger og anvendelse af netværkskrypstering. 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.

# Leverandøroversigt

**Fordeling af systemleverandører på specialer.**

Oversigten er baseret på yderregistret (data trukket af MedCom 2. september 2019). Oversigten bør dække alle former deltidspraksisser, herunder dem hvor man ikke har egen klinik og eventuelt er en del af et hus med flere specialer. For ni af klinikkerne er der ikke oplyst leverandør.

De markedsmæssigt største leverandører samarbejder i interessesammenslutningen PL – Primærsektorens Leverandørforum.

| Speciale | CGM XMO | EG Clinea | Novax | Win-PLC (a-data) | Ganglion (Aver & Lauritzen) | MultiMED | ClinicCare | MyClinic | Xmedicus | Patina | MedWin | RTGKOM | Formatex | Sum |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Anæstesiolog | | 9 | 5 | 7 | 2 | | 5 | 1 | 2 | 1 | | | | 32 |
| Røntgen* | | | | | | 6 | | 1 | 9 | | | | | 16 |
| Dermatolog | | 32 | 48 | 9 | | 1 | | | | | | | | 90 |
| Røntgen* | | | | | | | | | | | | 1 | | 1 |
| Reumatolog | 1 | 13 | 27 | 5 | 1 | | 1 | 1 | | | | | | 49 |
| Gynækolog | | 11 | 48 | | | 19 | | 1 | 1 | | | | 4 | 84 |
| Lunge og Allergi | | 11 | 11 | 11 | 5 | | 1 | 1 | | | 1 | | | 41 |
| kirurgi | | 15 | 29 | 7 | | 6 | 1 | | | | | | | 58 |
| Neurolog | 2 | 6 | 28 | | | 1 | | 2 | | | | | | 39 |
| Oftalmolog | | 70 | 70 | | 2 | 12 | | | | | | | | 154 |
| Ortopædkirurg | 1 | 13 | 12 | 2 | | | 2 | 1 | | | | | | 31 |
| Otolog | 6 | 80 | 11 | 47 | 1 | | 5 | | | | | | | 150 |
| Plastikkirurg | 1 | 3 | 8 | | | 2 | 1 | 2 | | | | | | 17 |
| Psykiater | 2 | 18 | 28 | 7 | 41 | 21 | 8 | 8 | | | | | | 133 |
| Pædiater | | 9 | 15 | 3 | 2 | | | 3 | | | | | | 32 |
| Børnepsykiatri | | 4 | | | 2 | 1 | 2 | 7 | | | | | | 16 |
| Alle specialer | 13 | 294 | 340 | 98 | 56 | 69 | 26 | 28 | 12 | 1 | 1 | 1 | 4 | 943 |

INDGÅR I ANALYSEN

MEDLEM AF PRIMÆRSEKTORENS LEVERANDØRFORUM

Deloitte.
Digital


## Jesper Kamstrup-Holm

Partner, Consulting
**Kontakt:** jesholm@deloitte.dk

## Thor Hvidbak

Senior Manager, Consulting
**Kontakt:** thvidbak@deloitte.dk

## Benjamin Vanggaard

Manager, Risk Advisory (Cyber)
**Kontakt:** benjjensen@deloitte.dk

## Nastasia Tørper

Seniorkonsulent, Consulting
**Kontakt:** ntoerper@deloitte.dk

## Vildana Amalie Coralic

Seniorkonsulent, Risk Advisory (Cyber)
**Kontakt:** vcoralic@deloitte.dk