POLITIK

Informationssikkerhedspolitik for Region Nordjylland

REGION NORDJYLLAND
– i gode hænder

INDHOLD

Indledning

Denne politik er Region Nordjyllands lokale supplement til den fællesregionale strategi for informationssikkerhed. Formålet med politikken er overordnet at beskrive hvordan Region Nordjylland arbejder med informationssikkerhed i dagligdagen.

Sikkerhed i Region Nordjylland

Når Region Nordjylland siger, at borgerne er *I gode hænder* gælder det ikke kun i det tidsrum, hvor de er i kontakt med sundhedsvæsenet. Når borgerne er i kontakt med Region Nordjylland, indsamles en række forskelligartede oplysninger hvoraf flere kan være personfølsomme. Indsamlingen sker som en naturlig del af regionens virke. Oplysningerne indsamles uanset om der er tale om patienter, borgere, pårørende, medarbejdere, samarbejdspartnere eller lignende, og om kontakten er i forbindelse med hospitalsbehandling, det specialiserede område, jordforurening eller noget helt fjerde. Regionen gør en stor indsats for at beskytte disse oplysninger, så de forbliver fortrolige og ikke kommer uvedkommende til kendskab. Oplysningerne skal altid være korrekte og ajourførte, og de skal være tilgængelige - men kun for de medarbejdere, der har brug for dem i løsningen af deres arbejdsopgaver.

Truslerne, mod de oplysninger regionen har om borgerne, er mangeartede og ændrer sig hele tiden. Derfor arbejder Region Nordjylland med sikkerhed efter anerkendte internationale standarder, som understøtter, at arbejdet sker effektivt og på et højt niveau. Regionens sikkerhedsarbejde kontrolleres og tilpasses løbende afhængig af truslerne – alt sammen for at beskytte borgernes oplysninger bedst muligt. Det kaldes i daglig tale **informationssikkerhed**.

Region Nordjyllands informationssikkerhedsprincipper omfatter ikke kun digitale oplysninger, men også f.eks. papirjournaler, blodprøver, røntgenbilleder og meget andet. Ligeledes gælder regionens sikkerhedsprincipper, når sundhedspersonalet mundtligt udveksler informationer om borgerne som et led i arbejdet, f.eks. på gangene på hospitaler eller ved konferencer.
Med andre ord skal borgerne kunne stole på, at følsomme personoplysninger om dem er *I gode hænder*.

Arbejdet med sikkerhed

I Region Nordjylland er arbejdet med sikkerhed opdelt i 14 områder og følger dermed sikkerhedsstandarden ISO27000. På den måde arbejdes der med alle relevante aspekter i det samlede sikkerhedsarbejde. Nedenfor kan du læse mere om de 14 områder.

Er der brug for yderligere information om sikkerhedsarbejdet, kan regionens Informationssikkerhedsafdeling kontaktes på informationssikkerhed@rn.dk.

Region Nordjyllands 14 sikkerhedsområder

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Personalesikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Overensstemmelse

Informationssikkerhedspolitikker

En af de grundlæggende forudsætninger for effektiv styring af Informationssikkerheden er, at der udarbejdes en overordnet politik for, hvordan informationssikkerhedsarbejdet tilrettelægges, organiseres, styres, evalueres, korrigeres og løbende kontrolleres. Politikken er godkendt af regionens ledelse og kommunikeres til medarbejdere og relevante samarbejdspartnere.

Politikken tager sit udspring i den fællesregionale Politik for Informationssikkerhed, og understøtter således Danske Regioners politiske linje for informationssikkerhed.

Politikken indeholder beskrivelser af de forskellige sikkerhedsområder og udmøntes i en række interne retningslinjer og instrukser, som både medarbejdere og samarbejdspartnere forpligter sig til at følge.
Politikken udstikker en række overordnede retningslinjer og krav indenfor de 14 områder og tildeler ansvarsområder til håndtering af sikkerhedshændelser, afvigelser og undtagelser.
Eksempler på interne politikker og retningslinjer er blandt andet

- Adgangsstyring
- Styring af aktiver
- Kodeord
- Mail
- Databehandleraftaler
- De registreredes rettigheder
- M.fl.

Organisering af informationssikkerhed

Det er både tids- og ressourcekrævende, at passe godt på borgernes oplysninger og derfor er det vigtigt, at ansvaret for informationssikkerheden i Region Nordjylland er entydigt forankret i regionens ledelse. Dette sikrer, at det overordnede sikkerhedsniveau i regionen afstemmes i forhold til den samlede økonomiske ramme og hensyn i regionen.

Region Nordjylland har etableret en informationssikkerhedsorganisation, som har til formål at skabe et ledelsesforankret grundlag for at kunne igangsætte og styre implementeringen af sikkerhedsinitiativer samt driften af informationssikkerhed i det daglige.

Regionsrådet

Regionsrådet er den øverste besluttende myndighed i informationssikkerhedsarbejdet. Regionsrådet træffer beslutning om sikkerhedsniveauet gennem den overordnede sikkerhedspolitik, og sørger for, at der stilles en afstemt økonomisk ramme til rådighed for informationssikkerhedsarbejdet.

Direktionen

Direktionen har det overordnede ansvar for at uddelegeringen af informationssikkerhedsopgaver i regionen, er i overensstemmelse med de rammer Regionsrådet har besluttet.

IT Direktøren

I Region Nordjylland binder IT-direktøren Informationssikkerhedsledelsen og Direktionen sammen samt sikrer et fornuftigt og praktisk beslutningsflow, så der kan eksekveres i et passende tempo.

Informationssikkerhedsledelsen (ISL)

Består af IT-direktør samt ledelsesrepræsentanter fra Informationssikkerhed, IT-sikkerhed samt IT Forvaltning, Drift og Support. ISL varetager og koordinerer den daglige ledelse af informationssikkerhedsarbejdet på taktisk plan og inddrages hvor der skal træffes hurtige beslutninger.

Udvidet informationssikkerhedsledelse (UISL)

Består af IT-direktør, ledelsesrepræsentanter fra Informationssikkerhed, Jura, IT-sikkerhed, IT Forvaltning, Drift og Support, Regionshospital Nordjylland, Aalborg Universitetshospital, Forskningens Hus og Psykiatrien. UISL varetager og koordinerer den daglige ledelse af informationssikkerhedsarbejdet på strategisk plan. Ledelsens tværfaglighed gør, at alle sikkerhedsaspekter i de forskellige dele af organisationen bliver identificeret. Ledelsen sikrer, at informationssikkerhedstiltag har den nødvendige effekt, samt vurderer og igangsætter informationssikkerheds- og privatlivsfremmende initiativer.

Databeskyttelsesrådgiver DPO

Regionens Databeskyttelsesrådgiver (DPO) har en rådgivende funktion i arbejdet med informationssikkerhed. DPO´ens funktion består i at rådgive, vejlede og overvåge at organisationen efterlever regler om databeskyttelse. DPO´en er kontaktled til Datatilsynet og samarbejder med Datatilsynet på vegne af Region Nordjylland.

Informationssikkerhedsteamet

Teamet består af to jurister, to IT-sikkerhedskonsulenter, to databeskyttelsesmanagere samt to informationssikkerhedskonsulenter. Teamet varetager den daglige drift af informationssikkerhedsarbejdet.

Teamets opgave er at understøtte og drive informationssikkerhedsarbejdet på tværs af hele organisationen. Teamet udarbejder blandt andet politikker, retningslinjer og instrukser og foretager løbende risikovurderinger.

Informationssikkerhedsambassadører

For at fremme og fastholde budskabet om at passe bedst muligt på borgernes oplysninger, har regionen udpeget ambassadører i alle sektorer og enheder. Ambassadørerne vil i samarbejde med databeskyttelsesrådgiveren sikre, at viden om en god og sikker håndtering af borgernes oplysninger når ud i alle hjørner af organisationen.

Personalesikkerhed

Det er vigtigt for Region Nordjylland, at medarbejdere, der indsamler, behandler eller på anden måde får, eller har adgang til borgernes oplysninger, forstår deres ansvar og har kompetencer til de roller, de er i betragtning til. Dette gælder både før, under og efter ansættelsen hos Region Nordjylland.

Før ansættelsen

Før ansættelsen foretager Region Nordjylland den nødvendige screening, hvilket f.eks. er indhentning af tilfredsstillende referencer samt verifikation af ansøgerens uddannelsesniveau og faglige kvalifikationer. Region Nordjylland tjekker altid autorisationen på sundhedsfagligt personale i forbindelse med nyansættelse. Der indhentes børneattester og straffeattester for de stillinger, hvor der i lovgivningen er hjemmel til at indhente attester. Skal medarbejderen have en særlig betroet rolle, kan det være nødvendigt med en særlig sikkerhedsgodkendelse – f.eks. hos PET.

Som et led i ansættelsesprocedurerne, skal alle medarbejdere acceptere tavshedspligterklæringer, før de kan få afgang til fortrolige og personfølsomme oplysninger.

Under ansættelsen

Når Region Nordjylland ansætter medarbejdere stilles der krav om, at de sætter sig grundigt ind i udvalgte politikker, retningslinjer, instrukser med videre, som vedrører regionens og lovgivningsmæssige sikkerhedskrav til håndtering af borgernes personoplysninger – og i særlig grad borgernes følsomme personoplysninger.

Det er den nærmeste leder, der i samarbejde med informationssikkerhedsorganisationen sørger for, at medarbejderne lever op til dette ansvar, og løbende bliver opdateret på, hvordan medarbejderne bedst muligt passer på borgernes oplysninger. Dette sker gennem løbende uddannelse og kampagner.

Hvis medarbejdere tilsidesætter sikkerhedskravene, kan regionen iværksætte en sanktionsproces, som tager hensyn til grovheden og arten af tilsidesættelsen, samt hvilken betydning den kan få for berørte borgere eller regionen.

Efter ansættelsen

Når en medarbejder stopper i regionen, gælder loyalitetspligten og tavshedspligten stadig. En fratrådt medarbejder, må ikke gemme, dele, nedskrive eller offentliggøre tavshedsbelagte oplysninger.

Samarbejdspartnere

Region Nordjylland samarbejder med en række eksterne personer og virksomheder, som ikke er ansat af regionen. Der stilles krav om at samarbejdspartnere, som behandler oplysninger for Region Nordjylland, skal underskrive en databehandleraftale, som oplister en række krav om hvordan oplysninger skal behandles. Hvis samarbejdspartneren udfører opgaver på regionens it-systemer uden at behandle data, så er det et krav, at der underskrives en virksomhedstavshedserklæring.

Styring af aktiver

Region Nordjylland vedligeholder et centralt register over alle aktiver, der kan lagre, registrere, opbevare, behandle, vise eller på anden måde anvende oplysninger om borgerne eller driften. Aktiver kan f.eks. være IT systemer, servere, printere, storskærme, telefoner eller medicoteknisk udstyr, som f.eks. scannere og meget mere. Registret har to formål:

1. At holde styr på alle de aktiver, som indkøbes og anvendes i den daglige drift i regionen. Herunder ligger fastlæggelse af ansvar, vedligehold, udskiftning og bortskaffelse.
2. At holde styr på, om udstyret indeholder informationer, som er følsomme eller kritiske for regionens daglige drift.

På den måde kan der skabes overblik over, hvordan udstyret skal beskyttes og det kan desuden dokumenteres, hvor følsomme oplysninger befinder sig.

Region Nordjyllands medarbejdere og samarbejdspartnere behandler regionens udstyr med størst mulig omhu i hele dets levetid. Ud over ovennævnte registre, er der udarbejdet en række interne retningslinjer og instrukser for, hvordan medarbejderne skal behandle oplysninger og aktiver. Det er instrukser for anvendelse af mobiltelefoner og tablets, anvendelse af PC'ere og instrukser for anvendelsen af medicoteknisk udstyr med videre. I instrukserne indgår der også anvisninger til, hvordan udstyret skal håndteres under transport, hvordan og hvornår det skal tilbageleveres og hvordan det skal behandles, hvis det skal genanvendes eller bortskaffes. Der kan være lagret oplysninger om borgere på udstyret, så derfor er det vigtigt med omhyggelig destruktion af alle informationer, inden det genanvendes eller bortskaffes.

Adgangsstyring

Formålet med adgangsstyring i Region Nordjylland er at sikre, at kun autoriserede brugere har adgang til regionens IT-systemer såvel som fysisk adgang, og samtidig, at uautoriseret adgang forhindres. Rammerne for adgangsstyring i Region Nordjylland er reguleret af gældende lovgivning.

For at kunne opretholde et højt informationssikkerhedsniveau, er det afgørende, at der er styr på hvem, der har adgang til hvilke elektroniske, såvel som ikke-elektroniske oplysninger, og hvornår der gives adgang, og med hvilke rettigheder. Adgangs- og brugerstyring er derfor et centralt og højt prioriteret område i det samlede arbejde med informationssikkerhed i regionen.

Det er Region Nordjyllands klare ambition til enhver tid at have de fornødne tekniske og administrative værktøjer til at sikre, at alle brugere, kun har de adgange og rettigheder, der er nødvendige for, at de kan varetage deres aktuelle arbejdsopgaver. Dette opnås blandt andet via regelmæssig kontrol af samtlige brugeres adgange til og rettigheder i regionens IT-systemer. Udover den periodiske kontrol

inddrages alle adgange og rettigheder, når brugerens ansættelsesforhold, kontrakt eller aftale ophører. I forbindelse med ændringer i ansættelsesforhold, der påvirker jobfunktionen, gennemgås alle rettigheder og adgange ligeledes.

Adgangsstyring i Region Nordjylland tager udgangspunkt i målsætningen om, at "det skal være let at gøre det rigtigt og svært at gøre det forkert", hvorfor der er særligt fokus på, at tilbyde brugervenlige IT-løsninger og supplerende dokumentation til processen med at oprette, vedligeholde og nedlukke brugere. Regionen har desuden en målsætning om, dels at begrænse antallet af brugere med administratorrettigheder (privilegerede rettigheder), og dels at begrænse, hvilke adgange og rettigheder disse har.

Udover styring af medarbejdernes adgange og rettigheder, er det afgørende, at regionens netværk er sikre og beskyttet mod uautoriseret adgang, således at borgere og medarbejdere kun har adgang til de netværk, som de er autoriserede til. På samme måde etableres der løbende adgangsstyring på udvalgte fysiske lokationer.

Region Nordjylland stiller en række konkrete krav til den enkelte bruger, blandt andet i forhold til brug af passwords og sikkerheden omkring passwords. Endvidere har regionen fokus på, at alle brugere kender reglerne for korrekt omgang med følsomme personoplysninger, således at reglerne i lovgivningen overholdes. Dette uanset om det foregår på det faste arbejdssted, eller en anden lokation. Region Nordjyllands politik for adgangsstyring er udmøntet i en række retningslinjer og instrukser, der samlet set dækker de relevante områder indenfor bruger- og adgangsstyring.

Kryptografi

Kryptografi er en effektiv metode til at beskytte oplysningers fortrolighed, intigritet og tilgængelighed. Når man krypterer oplysninger, ændrer man dem til en form, der gør dem ulæselige for uvedkommende. I Region Nordjylland anvendes kryptering i mange sammenhænge, både internt og eksternt ved udveksling af oplysninger via offentlige internetforbindelser. Det kan f.eks. være når regionen udveksler oplysninger via e-mail, som kaldes "Sikker mail". Dette kræver dog, at modtageren er i stand til at modtage og afkode oplysningerne. Hvis ikke dette er muligt, kan regionen sende oplysningerne på andre sikre måder – f.eks. ved hjælp af e-boks eller Digital Post, som er en krypteret og sikker digital kommunikationsform.

I en organisation som Region Nordjylland, er der personalegrupper, der har et arbejdsrelateret behov for at kunne tilgå borgernes oplysninger, mens de er på farten, arbejder hjemme eller har flexvagt. Der kan f.eks. opstå akutte situationer, hvor adgangen til oplysninger om borgerne er afgørende for, at regionen vil kunne give den rette behandling. Hvis medarbejderen med de rette kompetencer i en vagtsituation befinder sig på sin bopæl, er det vigtigt, at vedkommende kan få adgang til borgernes oplysninger på en sikker og autoriseret måde. Når medarbejderen logger på regionens systemer, sker det ved hjælp af kryptografiske værktøjer således, at oplysningerne ikke kan tilgås af uvedkommende undervejs fra serverne i regionens datacenter og ud til medarbejderens PC eller mobile enhed.

Kryptografi anvendes desuden til at sikre, at oplysninger på f.eks. bærbare PC´ere er krypterede. Dette sikrer, at fortrolige oplysninger, som måtte ligge på computeren, og som skal forblive fortrolige, ikke kan tilgås af andre end den bruger der logger på enheden.

Fysisk sikring og miljøsikring

Region Nordjylland har mange bygninger og faciliteter, med oplysninger og kritisk udstyr, som skal beskyttes mod forskellige typer af trusler.

Beskyttelsen skal bl.a. forhindre, at uvedkommende får uautoriseret fysisk adgang til sikre områder og skal samtidig forhindre beskadigelse og forstyrrelse af regionens oplysninger samt udstyr, som lagrer, behandler eller transmitterer oplysninger, eller som i øvrigt er væsentlige for den daglige drift. Sikre områder kan f.eks. være serverrum, regionens datacentre, lagerfaciliteter, kontorer, konferencelokaler, receptionsområder og behandlingsrum, hvori der befinder sig udstyr eller oplysninger som er personlige, kritiske eller nødvendige for den daglige drift.

Da mange af regionens bygninger og faciliteter er tilgængelige for offentligheden, giver det helt særlige betingelser for udformningen af sikkerheden. De fleste sikre områder kan beskyttes ved hjælp af mekanisk sikkerhed som f.eks. elektroniske låse på døre, som kun kan åbnes med adgangskort og/eller kode, låse på vinduer og døre, overvågningskameraer, alarmer med videre. Men ikke alle faciliteter kan sikres 100% mod fysisk uautoriseret adgang, fordi de skal være tilgængelige i akutte situationer, f.eks. behandlingsrum og operationsstuer. Der skal desuden være adgang for pårørende på hospitalerne.

Medarbejdernes adfærd har stor betydning for beskyttelse af borgernes oplysninger og regionens aktiver, som indeholder oplysninger. F.eks. skal regionen sørge for, at udstyr er behørigt rengjort og vedligeholdt. Udstyr må ikke fjernes uden forudgående registrering og tilladelse. Udstyr som, med tilladelse, benyttes udenfor regionens faciliteter skal sikres, f.eks. når udstyret medbringes i private køretøjer, eller benyttes i private boliger. Udstyr må ikke efterlades uden opsyn og medarbejderen skal være instrueret i sikker genbrug og bortskaffelse af udstyr.
Ud over den uautoriserede fysiske adgang til regionens faciliteter og medarbejdernes adfærd, beskyttes oplysninger og udstyr mod andre trusler som f.eks. brand-, strømafbrydelser, vandskader fra interne anlæg samt andre miljømæssige og udefrakommende hændelser som f.eks. storm, oversvømmelser, forurening, gasudslip med videre.

Endelig sikres oplysningers og kritiske funktioners fortsatte tilgængelighed gennem sikring af forsyninger af strøm og køling til regionens datacentre. Region Nordjyllands datacenter er Tier IV certificeret fra Uptime Institute, og efterlever dermed den højest mulige standard på området.

Driftssikkerhed

Region Nordjylland fokuserer på sikker, stabil og effektiv drift af IT-infrastruktur. Med IT-infrastruktur menes alt det udstyr, der binder regionens IT sammen i et stort sammenhængende netværk, fra centralt udstyr i datacentre, hvor servere og lagringssystemer findes, og helt ud til den enkelte PC og medicotekniske apparater på regionens mange lokationer. Endvidere omfatter IT-infrastrukturen al den software, der gør det muligt at afvikle egne forretningssystemer og den patientnære teknologi, så borgerne kan betjenes bedst muligt.

Den sikre, stabile og effektive drift kræver, at alle procedurer omkring drift af IT-infrastrukturen er formaliseret og tilgængelig for dem, der har brug for dem. Driftsprocedurer indeholder bl.a. svar på:

- Hvordan udstyr og systemer installeres, konfigureres og opdateres
- Hvordan der foretages sikkerhedskopier af oplysninger og software
- Hvordan overvågning af udstyr, systemer, oplysninger og trafik samt logning heraf gennemføres
- Hvordan fejl og usædvanlige hændelser håndteres
- Hvem der skal kontaktes ved fejl og hvordan systemer genetableres efter fejl.

Kort sagt dokumenteres driftsprocedurerne, hvordan der planlægges, udføres, evalueres og korrigeres på de opgaver som regionen løbende udfører, og på de fejl som opdages og rettes i dagligdagen.

Da IT-systemer løbende skal vedligeholdes og opdateres, f.eks. hvis der opdages sikkerhedshuller, som kan udnyttes af hackere eller nye funktioner, som er nødvendige for at gøre driften mere effektiv,

har regionen faste procedurer for, hvordan ændringer foretages. De fleste ændringer kræver grundig planlægning, og er der tale om større ændringer, placeres disse altid i servicevinduer. Det vil sige på planlagte og varslede tidspunkter, hvor tilretningerne forstyrrer driften mindst muligt. Forud for implementering af ændringer, sørges for, at ændringer er testet i separate test- og udviklingsmiljøer.

En af truslerne mod IT-infrastruktur, og dermed fortrolige oplysninger, er ondsindede angreb udefra. Regionen oplever jævnligt, at uautoriserede personer forsøger at trænge ind med det formål enten at stjæle, misbruge eller ødelægge oplysninger, eller placere ondsindet software som f.eks. virus, spyware, orme eller ransomware på regionens udstyr. Der opleves desuden jævnligt phishing-angreb, f.eks. hvor angriberen via e-mails forsøger at få medarbejdere til at klikke på links, som installerer uønsket software på udstyret. Derfor er der implementeret en lang række tekniske kontroller og tiltag, som har til formål at

- Forebygge, at uønsket software afvikles på regionens enheder
- Opdage, hvis skadelig software alligevel måtte blive forsøgt installeret og afviklet samt
- Udbedre effekterne af den skadelige software.

Foranstaltningerne mod skadelig software skal sikre Region Nordjylland mod tab og misbrug af data og oplysninger. Medvirke til at sikre stabilitet og sikre data og oplysningers korrekthed, tilgængelighed og fortrolighed.

Kommunikationssikkerhed

I Region Nordjylland handler kommunikationssikkerhed om at

1. beskytte Region Nordjyllands IT-netværk, som binder hele regionen sammen, og som både omfatter fiberforbindelser, kablede forbindelser og trådløse forbindelser
2. sikre, at medarbejdere er bevidste om, hvordan de skal kommunikere sikkert og uden fare for, at fortrolige oplysninger offentliggøres, eller falder i de forkerte hænder.

Dagligt transmitteres enorme mængder af oplysninger rundt på regionens IT-netværk mellem databaser, systemer, programmer, PC'ere, medicoteknisk udstyr med videre, og IT-netværket består samlet set af flere tusinde enheder. Det er derfor vigtigt, at styre, kontrollere og løbende opdatere netværksenheder og -forbindelser, for at beskytte data og oplysninger bedst muligt.

Da IT-netværket er den eneste vej til borgernes oplysninger kræver det, at sikkerheden prioriteres højt, og at der etableres passende sikkerhedsforanstaltninger med tilhørende løbende kontrolforanstaltninger for at sikre tilgængelighed, fortrolighed og korrekthed af data og oplysninger. Styringen varetages af et højt specialiseret IT-driftsteam, der ved hjælp af faste procedurer, sikrer rutinerne omkring den daglige drift. Dette gælder både ved anskaffelse, drift, vedligeholdelse, opdateringer, udskiftninger med videre samt ved håndtering af hændelser.

Adgang til regionens IT-netværk sker gennem sikkerhedsgodkendte adgangskontrolløsninger og trafikmønstre på IT-netværket logges. Regionen benytter systemer,

- der kan advare og alarmere, hvis der konstateres uønsket eller mistænkelig trafik og adfærd.
- der kan afvise adgangen til enheder, som regionen ikke kender, eller som ikke burde være tilsluttet IT-netværket.
- der kan afvise kommunikationen mellem enheder, som regionen ikke kender, eller som ikke burde være tilsluttet IT-netværket.

For at kunne opdage og minimere angreb fra internettet, er der installeret beskyttende systemer foran regionens datacentre samt alle systemer og programmer, der kan tilgås fra internettet. Systemerne tillader kun trafik, som er forretningsmæssigt begrundet.

Når fortrolige oplysninger overføres, både internt i regionen, og til og fra eksterne parter som f.eks. Sundhedsdatastyrelsen eller andre samarbejdspartnere, er der etableret systemer og teknologier, der beskytter oplysningerne mod aflytning, kopiering, ændringer, fejlforsendelse og ødelæggelse, destruktion og sletning.

Vores medarbejderes bevidsthed om, hvordan de skal kommunikere både internt og eksternt, f.eks. om borgere eller andre, er ligeledes vigtigt og højt prioriteret hos Region Nordjylland. Medarbejderne instrueres blandt andet i

- Kommunikation via sikker e-mail
- Hvad man skal være opmærksomme på ved modtagelse af e-mails (afsendere, links med videre)
- Hvor længe e-mails og andre dokumenter må opbevares
- Hvordan og hvor fortrolige samtaler må afholdes
- Hvordan dokumenter og filer med oplysninger om borgerne udveksles, og hvor de må gemmes
- Regler om, at medarbejdere ikke indtaler beskeder, som indeholder personlige informationer om borgerne, på telefonsvarer.
- At medarbejdere ikke bruger SMS som kommunikationskanal/behandlingskanal, men kun til aftalepåmindelser

Anskaffelse, udvikling og vedligeholdelse af systemer

Region Nordjylland har mange forskellige IT-systemer, som hjælper med at understøtte det daglige arbejde med at betjene borgerne bedst muligt og mest effektivt. Da den teknologiske udvikling i sundheds-IT går meget hurtigt, er det nødvendigt at have præcise og klare rammer for anskaffelse, udvikling og vedligeholdelse af systemerne.

Alle sikkerhedsaspekter i både nye og eksisterende systemer skal analyseres og vurderes inden der enten anskaffes nye systemer, udvikles nye eller udvikles og optimeres på eksisterende systemer. Analyserne skal afdække, i hvilken grad systemet kan håndtere oplysningers fortrolighed, korrekthed og tilgængelighed. Hvis der indgår personoplysninger i systemet, udføres desuden en analyse af risici for den registrerede, f.eks. borgeren, inden systemet sættes i drift eller ændringerne foretages.

Databeskyttelse skal være designet ind i regionens løsninger, f.eks. gennem adgangsstyring, dataminimering, pseudonymisering med videre. Indstillinger i IT-systemer, som sikrer, at kun nødvendige oplysninger kan tilgås, skal være slået til som standard.

Region Nordjylland arbejder struktureret med ændringsstyring efter internationale standarder, og ingen nye store systemer sættes i drift og ingen store ændringer foretages med mindre de er grundigt testet i beskyttede testmiljøer og alle obligatoriske analyser er udført og dokumenteret. I testen indgår bl.a. krav til adgangstildeling, systemgrænseflader og integrationer med andre systemer. Dette er uanset, om udviklingen eller vedligeholdelsen foretages af Region Nordjylland eller af leverandører – der stilles helt samme krav til tests og analyser, som skal dokumenteres.

Leverandørforhold

Region Nordjylland benytter et meget stort antal eksterne leverandører, som alle er med til at få dagligdagen i regionen til at fungere bedst muligt. Flere af leverandørerne har adgang til regionens informationer herunder personoplysninger, systemer (aktiver) og faciliteter, som en naturlig del af samarbejdet. Dette kan udgøre en risiko for informationssikkerheden, og det er derfor nødvendigt, at regionen identificerer og definerer, hvordan regionen og leverandørerne skal håndtere sikkerhed og beskytte informationer og aktiver, gennem hele samarbejdet.

Regionen vurderer leverandører inden et samarbejde indledes. Vurderingen afhænger af samarbejdets art og omfang, og kan f.eks. resultere i, at leverandøren skal dokumentere, at leverandøren som minimum efterlever samme sikkerhedsniveau og –krav, som regionen selv ønsker at efterleve. Hvis leverandøren skal behandle personoplysninger, skal leverandøren underskrive en databehandleraftale, som forpligter leverandøren til at efterleve både lovgivningskrav samt regionens interne sikkerhedskrav. I databehandleraftalen vil det fremgå, hvilke typer og kategorier af personoplysninger leverandøren behandler, samt hvordan og til hvilket formål leverandøren må og skal behandle dem. Anvender leverandøren underleverandører, vil underleverandøren skulle efterleve samme krav.

Hvis leverandører har adgang til personoplysninger uden der er tale om en databehandlersituation, skal der underskrives en tavshedserklæring, som forpligter leverandøren til at hemmeligholde alle informationer som leverandøren og dennes ansatte kommer i besiddelse af eller får kendskab til, både under og efter samarbejdet.

Region Nordjylland fører tilsyn med leverandører og eventuelle underleverandører, hvis disse behandler personoplysninger på vegne af os. Tilsynet er f.eks. kontroller, der er iværksat for at kunne evaluere på sikkerhedsniveauer, herunder adgangsstyring, gennemgang af resultater, overvågning, logning, rapportering og audit samt krav til nødsituationer og beredskab. I visse tilfælde vil et tilsyn være suppleret med et krav om yderligere dokumentation, f.eks. revisionserklæringer, som dokumenterer leverandørens sikkerhedsniveau samt opnåelsen heraf.

Styring af informationssikkerhedsbrud

Region Nordjylland investerer mange ressourcer i at sikre personoplysninger om borgere, på trods af det så vil det aldrig være muligt 100% at undgå uforudsete hændelser. Region Nordjylland har blandt andet fokus på teknisk og organisatorisk sikkerhed, herunder uddannelse af medarbejdere i sikker og forsvarlig håndtering af personoplysninger og fortrolige oplysninger.

Region Nordjylland forbereder sig bedst muligt til de situationer, hvor skaden alligevel måtte opstå. Region Nordjylland anvender internationale best practice standarder for informationssikkerhed og arbejder løbende på at sikre at krav og rettigheder i blandt andet EU persondataforordningen overholdes. På denne måde kan regionen begrænse virkningerne af sikkerhedsbrud.

Et brud på informationssikkerheden opstår når en hændelse påvirker fortrolighed, korrekthed og/eller tilgængelighed for oplysninger om borgerne.

Et brud på informationssikkerheden kan opstå, når IT-udstyr har været skyld i, eller været direkte indblandet i, bruddet. Det kan f.eks. være, hvis et hackerangreb trænger gennem regionens sikkerhedssystem, og forsøger at stjæle, blokere eller ødelægge oplysninger, eller hvis en ellers gennemtestet opdatering af et kritisk system, mod forventning, skaber utilgængelighed af personoplysninger om borgerne, for regionens medarbejdere.

Sikkerhedshændelser kan også opstå, hvis en medarbejder bryder sin tavshedspligt og fortæller uvedkommende om borgere eller regionens drift, eller hvis regionens faciliteter bliver gjort utilgængelige eller begrænsede som følge af brand-, storm- eller vandskader.

Region Nordjylland har klare procedurer for håndtering af brud på informationssikkerheden, med det formål at begrænse dem mest muligt, og understøtte at de er til mindst mulig gene for patienter, samarbejdspartnere og medarbejdere.

Indenfor alle typer af brud er det væsentligt om personoplysninger er omfattet, og om bruddet kan eller vil få konsekvenser for borgerne. Afklaringen er vigtig, fordi der i sådanne tilfælde stilles særlige krav til håndteringen og eventuel anmeldelse til Datatilsynet og underretning af de berørte borgere. Informationssikkerhedsbrud, der samtidig er brud på persondataforordningen håndteres af Region Nordjyllands databeskyttelsesrådgiver.

I forbindelse med et brud sørger regionen for at indsamle de relevante oplysninger om hændelsen – både for at sikre dokumentation til brug for eventuel senere undersøgelse, men også til brug for efterfølgende iværksættelse af korrigerende tiltag. Dette med henblik på at mindske risikoen for, at lignende situationer opstår.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Som en overbygning på den strukturerede hændelseshåndtering har Region Nordjylland etableret beredskabsplaner, som sikrer, at planer for de forskellige dele af organisationen er sammenhængende og tilgodeser alle sikkerhedskrav og samtidig fastlægger prioriteringen af afprøvning og vedligeholdelse.

Beredskabsplanerne er væsentlige fordi de præciserer, hvordan regionen skal agere, når den normale drift er sat ud af spil. Det vil sige hvem gør hvad og hvornår, og hvordan sikres det, at normal drift kan genoprettes hurtigst muligt. Formålet med beredskabsplaner er således, at begrænse konsekvenserne ved en katastrofe eller større nedbrud til et acceptabelt niveau, samt at være i stand til at genoprette hurtigst muligt gennem udbedrende foranstaltninger, og herefter etablere forebyggende foranstaltninger.

Som en forebyggende foranstaltning, udføres løbende risikovurderinger af trusler mod regionen og driften, så organisationen er bedst muligt forberedt, hvis katastrofen måtte ramme. Risikovurderingerne har et særligt fokus på regionens kritiske funktioner og IT systemer, som er vitale i forhold til at beskytte borgerne og deres informationer bedst muligt.

Beredskabsplanerne er omfattende, og indeholder bl.a. klare definitioner af, hvornår beredskabet aktiveres, hvem der involveres, hvad der forventes af dem og hvem der skal notificeres – og hvornår.

For at sikre, at beredskabsplanerne har den nødvendige effekt, afprøves beredskabet løbende. Dette giver både borgere, medarbejdere og samarbejdspartnere den fornødne tryghed for, at alle er trænet i og bekendt med deres roller og ansvar i beredskabet, og at det altid er tilpasset de trusler regionen står overfor som leverandør af sundhedsydelser.

Overensstemmelse med lov- og kontraktkrav

Regionens hovedopgave er at drive det nordjyske sundhedsvæsen. Regionen har desuden et overordnet ansvar for den regionale udvikling og tager sig også af specialiserede opgaver på det sociale område.

Med dette følger ikke bare et stort ansvar, men også et krav om, at overholde en lang række regler, som er beskrevet i lovgivningen eller som følger af generelle eller specifikke myndighedskrav.
I arbejdet med Informationssikkerhed, har regionen et overblik over, hvilke love og regler der gælder. I forhold til informationssikkerhedsarbejdet gælder f.eks.

- Databeskyttelsesforordningen
- Databeskyttelsesloven
- Forvaltningsloven
- Offentlighedsloven
- Sundhedsloven
- Serviceloven
- Lov om klage og erstatningsadgang
- Lov om markedsføring af sundhedsydelser
- Blodforsyningsloven
- Vævsloven
- Retssikkerhedsloven
- Logningsbekendtgørelsen
- Arkivloven

Ud over lovgivningen indgås løbende aftaler med samarbejdspartnere, hvori der indgår en række aftalevilkår, som regionen er forpligtet til at efterleve.

Når vi indgår en kontrakt eller en juridisk bindende aftale, sikrer vores juridiske afdeling, eksempelvis i komplicerede sager eller sager med betydelig økonomisk værdi, at eventuelle myndighedskrav og regionens interne sikkerhedskrav er overholdt. Ved mindre og ukomplicerede sager, håndteres aftalerne typisk lokalt.

En væsentlig del af regionens virke i sundhedssektoren beror på forskning og forskningsresultater. Det er vigtigt, at regionen ikke krænker tredjemands enerettigheder til disse resultater, hvis andre er fremkommet til samme resultater tidligere. På samme måde er regionen en stor organisation med mange medarbejdere, og det er også vigtigt, at ingen kopierer, downloader eller på anden måde anvender digitalt eller fysisk materiale, som andre har rettighederne til.

Endvidere består det daglige arbejde i behandlingen af personoplysninger om bl.a. borgerne. Behandlingen af disse personoplysninger er underlagt strenge regler, som regionen lægger et stort arbejde i at efterleve. Bl.a. stiller Databeskyttelsesforordningen og -loven krav til, at behandlingen af borgernes oplysninger kun må anvendes til udtrykkelige og rimelige formål. Efterfølgende behandling af borgernes oplysninger må ikke være uforenelig med de oprindelige formål.

Behandlingen af personoplysninger må ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvor til oplysningerne indsamles.

Personoplysningerne må ikke opbevares i længere tid end nødvendigt og må ikke anvendes til andre formål end det angivne, med mindre den, som oplysningerne handler om, giver sit udtrykkelige samtykke til det. Regionen sikrer sig, at personoplysninger er korrekte og ajourførte, og har implementeret procedurer for, at ukorrekte oplysninger korrigeres.

Regionen har implementeret procedurer for, hvordan en indsigelse fra borgerne mod behandling af personoplysninger håndteres.

Borgerne har til enhver tid ret til at anmode om at få indsigt i egne personoplysninger, der indsamles og behandles af regionen.

Som borger har man endvidere til enhver tid ret til, at få udleveret information om egne oplysninger som indsamles og anvendes i regionens daglige arbejde.

Hvis regionen overfører personoplysninger til lande uden for EU, må det kun ske, hvis der er et særligt retligt grundlag for det.

Informationssikkerhedspolitik for Region Nordjylland

Informationssikkerhed
Niels Bohrs Vej 30
9220 Aalborg Øst

27. maj 2019

REGION NORDJYLLAND
– i gode hænder