Personvern og informasjonssikkerhet, særlig etter GDPR

Læringsmål nr 44:
Kjennskap til sentrale vilkår for personvern og informasjonssikkerhet. Her under personvernlovgivningen, sikker pålogging, autentisering, loggføring, sikker meldingsutveksling og prinsippet for meldingskvitteringer.

Jurist Grete K Nielsen

Fylkesmannen i Oslo og Viken

23.10.2020

Hva er personvern ?

- Definisjon:
  - «Enkelt sagt handler personvern om retten til et privatliv og retten til å bestemme over egne personopplysninger».

    (Datatilsynet)
- Personopplysninger
  - Opplysninger som kan knyttes til en enkeltperson. Både:
    - Direkte identifiserende (med navn)
    - Indirekte identifiserende (kodede)
  - Særlig kategori
    - Rasemessig eller etniske bakgrunn, straffbare forhold, helseforhold, seksuelle forhold og medlemskap i fagforening

Foto:

Personvern og menneskerettigheter

Den europeiske menneskerettighetskonvensjon (EMK) artikkel 8

"Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.»

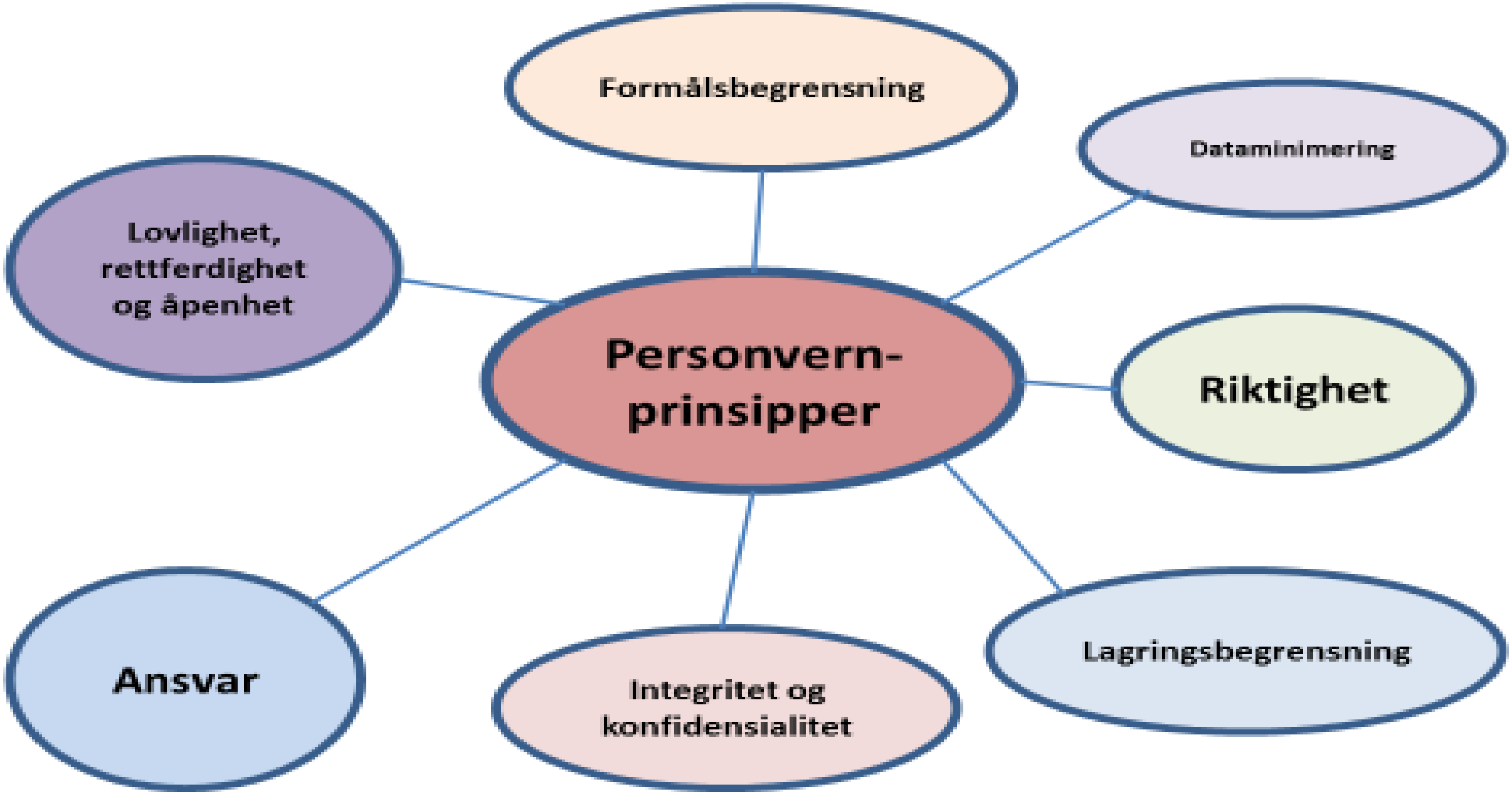
Grunnloven § 102 (13. mai 2014):

"Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.

Statens myndigheter skal sikre et vern om den personlige integritet

Rettslige rammer

- GDPR/Personvernforordningen
- Ny personopplysningslov
- Helseforskningsloven
- Helseregisterloven m/forskrifter
- Annet internasjonalt regelverk


Formålsbegrensning
Dataminimering
Lovlighet, rettferdighet og åpenhet
Personvern-prinsipper
Riktighet
Ansvar
Integritet og konfidensialitet
Lagringsbegrensning

Rettigheter - Plikter

Rett for én

«den registrerte»

- Informasjon – (hvordan og hvorfor -tydelig forklart!)
- Innsyn
- Korrigering (uriktige opplysninger) - forutsetter innsyn!
- Sletting / "retten til å bli glemt" (uten ugrunnet opphold)
- Behandlingsbegrensning (for eks. sperremekanismer – data "fryses", kan ikke behandles / endres)
- Protest (tungtveiende årsaker hos den registrerte)
- Dataportabilitet (automatiserte opplysninger – kommer fra den registrerte og er samtykkebasert – f.eks: forsikring, mobil abn. etc.)
- Rettigheter for de registrerte (GDPR art. 14-23)

Plikt for en annen

«behandlingsansvarlig»

- Konfidensialitet og integritet (art. 5 nr. 1 f), hindre uautorisert tilgang og ødeleggelse v/ organisatoriske og tekniske tiltak
- Lagringsbegrensning (art. 5 nr. 1 e), tid!
- Formålsbegrensning (art. 5 nr. 1 b), til hva?
- Dataminimering (art. 5 nr. 1 c), hva trenger vi?
- Kvalitet/riktighet (art. 5 nr. 1 d), helseregistre!
- Dokumentasjon/oversikt (art. 30)
- Sikkerhetstiltak (art. 32) - egnet sikkerhetsnivå!
- https://www.ba.no/bergen-kommune/nyheter/skole-og-utdanning/foreldre-med-besoksforbud-lagt-til-i-skole-app/s/5-8-1151953

Viktige endringer og nyheter i 2018: GDPR

- Like regler i alle EU land.
- Forsterkede internkontrollplikter:
  - Vurdering av personvernkonsekvenser (DPIA)
  - Innebygd personvern (Data protection by design and by default)
  - Personvernombud obligatorisk for offentlige og noen andre virksomheter
- Nye og skjerpede rettigheter
  - informasjon og samtykke
  - dataportabilitet
  - Sletting
  - Varsling av registrerte ved sikkerhetsbrudd
- Strengere sanksjoner (20 M Euro / 4 % av årlig omsetning)
- Brudd på personopplysningssikkerheten skal meldes til Datatilsynet (art. 33) innen 72 timer.

Hva er personopplysningsvern?

- «Den enkeltes rett til å ha kontroll med egne personopplysninger»
- Selvbestemmelse
  - Rett til selv å bestemme hvilke opplysninger som skal brukes, av hvem, til hvilke formål osv.
- Informasjon
  - Hvis man ikke har rett til å samtykke, har man i det minste rett til å vite hvilke opplysninger som skal brukes, av hvem, til hvilke formål.
- Personvern dreier seg om personlig integritet, privatliv, selvbestemmelse og selvutfoldelse
  - Mer enn personopplysningsvern
  - Mer enn informasjonssikkerhet

EUs GDPR og norsk lov innen helse

- Norsk helselovgivning tilfredsstiller alle kravene i EU sin GDPS lov, bortsett fra pålegg om personvernombud.
    - HOD viser til at det ikke er behov for generelle hjemler for behandling av helseopplysninger når man yter helsehjelp.
    - Prop. 56 LS (2017-2018) s. 184-185, se også side 44-45
- Ansvarsforhold:
    - Helseforetakene
        - Databehandlingsansvarlig
        - Ansvarlig for å tilrettelegge for forsvarlige tjenester
    - Helsepersonell
        - Forholde seg til HPL og PasRL

Personvern i helse: juss + politikk + medisin

- Balansere: behovet for samhandling – personvern:
  - Er IKT-systemene gode nok for dette?
- HOD i rundskriv 14. april 2019 problematiserer dette
  - «Forholdet mellom pasientsikkerhet og den enkeltes personvern er balansert på et overordnet nivå i regelverket.»
  - «Reglene må forstås og praktiseres i lys av at gode helsetjenester forutsetter at relevante pasientopplysninger kan deles. Helsepersonell har behov for opplysningene til å gi helsehjelp, til å kvalitetssikre helsehjelpen som gis og til egen læring.»

Personvernloven og GDPR innen helsehjelp

- Personvernloven/GDPR (personvernregelverket) gjelder personopplysninger på alle områder i samfunnet
- Yter helsehjelp:
  - Helselovgivningen gjelder for helseopplysningene og i store trekk dekker de kravene til personvernloven på dette feltet.
  - Innenfor helseretten: lange tradisjoner og omfattende reguleringer knyttet til forsvarlighetsplikt, plikt til taushet, opplysningsrett- og plikt, dokumentasjonsplikt (helsepersonelloven)
- Ikke yter helsehjelp:
  - Helselovgivningen gjelder for helseforskning: helseforskningsloven og helseregisterloven.
    - Eksempel: forskning på helseopplysninger, helseregister, IT systemer, økonomi oversikter mm

Personvern i helsesektoren: «Normen»

Styringsgruppe

- Avtale
  - forpliktende og referer til lovkrav.
- Mellom
  - de fleste av sektorens virksomheter (> 10 000) og deres leverandørers og databehandlere.
- Regulerer
  - sikker pålogging, autentisering, loggføring, sikker meldingsutveksling og prinsippet for meldingskvitteringer

Daglig sekretariat

Direktoratet for e-helse

norskhelsenett

Taushetsplikten
- blir personvernhensyn ivaretatt?

- Plikt for helsepersonell, rettighet for pasienter
- Gjelder mellom pasient og behandler- nødvendighetskrav
- Utfordres stadig av nye krav til tilgjengelighet som følge av
    - Teknologisk utvikling
    - Organisering av helsetjenesten
    - Rapporteringskrav
    - Meldingsplikt
    - Arkivplikt
    - Kjernejournal
    - En innbygger- en journal
    - Helseforskningsloven- utlevering til forskningsformål
    - Sekundærbruk av helseopplysninger
    - Bruk av eksterne tjenesteleverandører/ databehandlere
    - Digitale hjelpemidler
    - Automatiserte tjenester
    - Behandlingsstøtteverktøy

Utfordringer forts..

- Digitalisering
- Deling på tvers
- Pasientflyt primær og spesialisthelsetjeneste
- Taushetsplikt
- Informasjonsplikt og rett
- Reservasjonsrett- rett til sperring
- Tilgjengelighet- krav og forventning
- Frykt for og forebygging mot «snoking»
- Ytre trusler- fremmede makter- motivasjon?
- Verdien av helseopplysninger
- Formålsutglidning
- Informasjon
- Samtykke
- Tjenesteutsetting

Hvordan er personvernkonsekvensene vurdert?

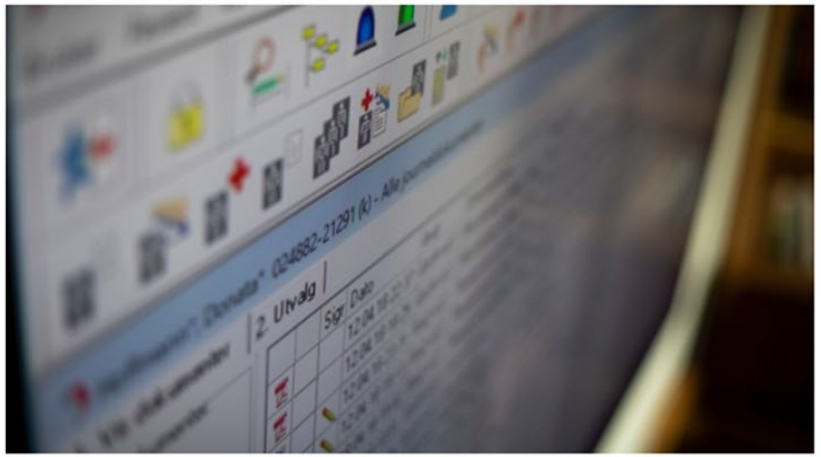
- Personvernhensyn vil bli ivaretatt gjennom
  - informasjonssikkerhetstiltak som tilgangskontroll og logg

- I media:
  - Individnivå: trusselbildet= snoking?
    - Tiltak=taushetsplikt, logg og identitetsforvaltning /tilgangskontroll
  - Systemnivå:
    - Regulering av IKT systemer for å motvirke cyberkriminalitet bra nok? jf. IKT-skandalen i Helse Sør Øst
    - Rutiner og opplæring intern for personvern bra nok? jf postliste skandalen på sykehusene nylig?

Snoking

Ansatt tatt i snoking – 60 pasienter berørt

En medarbeider ved Dalane distriktspsykiatriske senter er tatt for å ha snoket i pasientjournaler. Rundt 60 pasienter er berørt.



Pasientjournalsystemet Dips brukes ved alle norske helseforetak unntatt Helse Midt-Norge. På bildet ser vi en testversjon av systemet. Her kommer det ikke fram noen ekte pasientopplysninger.
FOTO: ROLV CHRISTIAN TOPDAHL / NRK

Rolv Christian Topdahl
@rolvc
Journalist

Publisert 7. feb. kl. 14:08
Oppdatert 7. feb. kl. 19:55

– En blir nesten ordløs, sier Målfrid J. Frahm Jensen.

Hun er tidligere erfaringskonsulent på psykiatrisk klinikk på SUS. I 16 år har hun kjempet mot snoking i pasientjournaler.

– For sykehuset sier gang på gang at pasientene må ha tillit til dem og ha tillit til personvernet. Likevel så skjer det gang på gang at helsepersonell blir tatt i snoking, sier Frahm Jensen.

Hun spør hvordan en da kan ha tillit til helsetjensten - spesielt psykiatrien:

– Der du forteller om de mest sensitive og skambelagte ting, og så sitter andre og leser dette. For noen av disse pasientene føles dette som et overgrep.

Mange pasienter blir lagt inn på ny: – Kunne vært unngått

Pasientjournalen var sperret for akkurat ham – snoket likevel

Pasienten mente legens behandling var uforsvarlig. Hun sperret derfor journalen sin for ham. Men legen snoket likevel. Nå er frykten at dette kan skje flere steder.

Stavanger universitetssjukehus (SUS) får refs av Helsetilsynet for at legen i det hele tatt hadde tilgang til den sperra journalen.
FOTO: ØYSTEIN OTTERDAL / NRK

Rolv Christian Topdahl
@rolvc
Journalist

Publisert 21. juni 2019 kl. 07:55
Oppdatert 21. juni 2019 kl. 13:28

Artikkelen er mer enn ett år gammel.

– Det var veldig, veldig ubehagelig.

Det sier kvinnen, som ønsker å være anonym. Hun har vært ut og inn av psykiatrien i flere år. Hun lider blant annet av en alvorlig post traumatisk stresslidelse.

I desember 2014 sperret kvinnen journalen sin for innsyn. Og i sperre-søknaden nevnte hun spesielt sin tidligere lege og behandler ved psykiatrisk klinikk ved Stavanger universitetssjukehus.

Kvinnen ville ikke at overlegen skulle ha noe med henne å gjøre mer. Grunnen var dette:

Forskarar fryktar ny bølgje av hjarte- og karsjukdom

IKT systemer

- Legene må forutsette at systemansvarlig tilrettelegger for trygge systemer
- Datatilsynet fant lovbrudd: Millionbøter etter outsourcing av sykehus-IT
    - Rapport: Flere lover ble brutt og det ble gjort mangelfulle vurderinger av sikkerhet og risiko før Helse Sør-Øst vedtok å outsource IT-infrastrukturen.

https://www.nrk.no/norge/millionboter-etter-outsourcing-av-sykehus-it-1.13751516

https://www.digi.no/artikler/helse-sor-ost-skroter-milliardavtale-om-utflagging-av-it/439971

OUTSOURCING

Helse sør-øst skroter milliardavtale om utflagging av IT

Styret i Helse sør-øst har bestemt seg for å droppe milliardavtalen om å outsource IT-systemene i helseforetaket.

Ullevål Sykehus (illustrasjonsfoto). (Bilde: NTB scanpix)

NTB HELSE-IT 14. JUNI 2018 - 19:16 ENDRET 15. JUNI 2018 - 08:47

Facebook Twitter Linkedin

Styret i Helse sør-øst opplyser i en pressemelding at hele kontrakten om utflagging av IKT-infrastruktur med selskapet DXC avbestilles.

Det er ett år siden NRK avslørte at IT-arbeidere i blant annet Malaysia, India og Bulgaria hadde tilganger til pasientdata, selv før formell overtakelse av IT-systemene. Dette var i strid med alle løfter som var gitt til Stortinget, og umiddelbart ble hele avtalen satt i bero.

På et styremøte torsdag ble det vedtatt at man nå skal skrote hele avtalen, noe som trolig kommer til å koste dyrt. Det er helseforetaket Sykehuspartner HF, som har hatt ansvar for kontrakten.

Datatilsynet fant lovbrudd: Millionbøter et outsourcing av sykehus-IT

Flere lover ble brutt og det ble gjort mangelfulle vurderinger av sikkerhet og risiko før Helse Sør-Øst vedtok å outsource IT-infrastrukturen. Det slår Datatilsynet fast i en ny rapport.

LOVEN GJELDER IKKE FOR ALLE: Disse damene stod i spissen for outsourcingen. Adm. direktør Cathrine Lofthus og styreleder Ann Kristin Olsen får kritikk for manglende styring og ledelse, men er ikke omfattet av samme lovverk som sykehusene og Sykehuspartner. Derfor slipper Helse Sør-Øst RHF bøter.

FOTO: ANNE CECILIE REMEN / NRK

Line Tomter
Journalist

Anne Cecilie Remen
Journalist

Publisert 27. okt. 2017 kl. 07:26
Oppdatert 19. jan. 2018 kl. 19:00

Artikkelen er mer enn to år gammel.

> *Vår vurdering er at det ikke finnes formildende omstendighet i denne saken*
>
> DATATILSYNET

I en rapport helseforetakene i Helse Sør-Øst mottok torsdag ettermiddag felles en knusende dom over mangelen på risikovurdering i forkant av IT-outsourcingen

Sykehustabbe: UNN la ut sensitive pasientopplysninger på nett

Ved en feil la sykehuset UNN ut personopplysninger i 95 taushetsbelagte saker på internett. Opplysningene ble liggende i nesten to døgn. Datatilsynet sier hendelsen er alvorlig.

Landsdelens største sykehus la ved en feil ut sensitive personopplysninger åpent på nett i sin postjournal.

FOTO: JØRN INGE JOHANSEN / NRK

Elise Holdal
@EliseHoldal
Journalist

Publisert 13. mai kl. 17:14

https://www.nrk.no/tromsogfinnmark/unn-la-ut-sensitive-personopplysninger-pa-nett_-_-alvorlig-1.15015856

Oslo universitetssjukehus beklagar publisering av personnummer og pasientnamn i postlista

Sjukehuset skriv at det er sterkt beklageleg og at slikt ikkje skal skje.

Oslo universitetssjukehus er lokalsjukehus for store delar av Oslo si befolkning. Dei driv mellom anna OUS Ullevål.

FOTO: FREDRIK VARFJELL / NTB SCANPIX

Hans Ivar Moss Kolseth
Journalist

Helge Carlsen
Journalist

Andreas de Brito Jonassen
Journalist

Pedja Kalajdzic
Journalist

Katarina Poensgen
Journalist

Publisert 19. mai kl. 12:01
Oppdatert 19. mai kl. 21:55

I ei pressemelding skriv Oslo universitetssjukehus at dei har oppdaga at 275 personnummer «og/eller» pasientnamn har blitt publiserte på sjukehuset si offentlege postliste dei siste tre åra.

– Vi fekk varsel fredag kveld frå ein ekstern aktør om at vi hadde fleire journalpostar med fødselsnummer og namn liggande ute i vår offentlege postjournal, seier direktør for Oslo sykehusservice, Geir Tangstad, til NRK.

Sjølve dokumentet var ikkje tilgjengeleg på nett, men det har vore mogleg å lese namn og personnummer ut frå opplysningane i journalen. Postlistene skal vere midlertidig fjerna frå sjukehuset sine nettsider. Saka vert følgt opp internt og varsla til Datatilsynet.

– Rutinen har vore at ein går gjennom postlistene manuelt for å sikre seg at eventuelle namn eller personnummer ikkje blir publisert. Det er i denne manuelle gjennomgangen det har svikta i desse tilfella, seier Tangstad.

https://www.nrk.no/norge/oslo-universitetssjukehus-publiserte-275-personnummer-og_eller-pasientnamn-i-postliste-1.15022690

Offentlig debatt: forskning – personvern

Fylkesmannen i Oslo og Viken

23.10.2020

FOTO: Jon Olav Nesvold / NTB scanpix BILDETEKST

Forsøket på å fremstille personvern og pasientsikkerhet som motsetninger er uheldig.

BJØRN ERIK THON
DIREKTØR I DATATILSYNET
CAMILLA NERVIK
FAGDIREKTØR, DATATILSYNET

27. DES. 2018 19:00 10:31

Sykehuset ivaretar både pasientsikkerhet og personvern | Sølvi Andersen

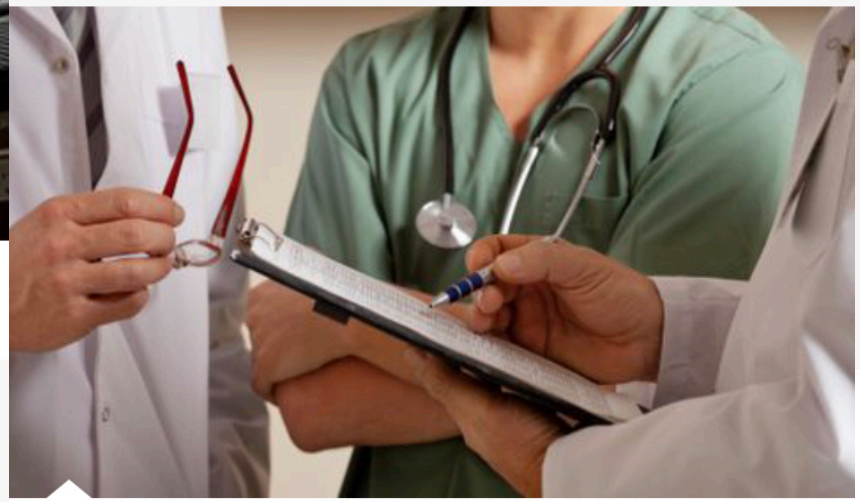


FOTO: Shutterstock, NTB Scanpix BILDETEKST

I den pågående debatten i Aftenposten kan man få inntrykk av at personvern står i veien for pasientsikkerheten.

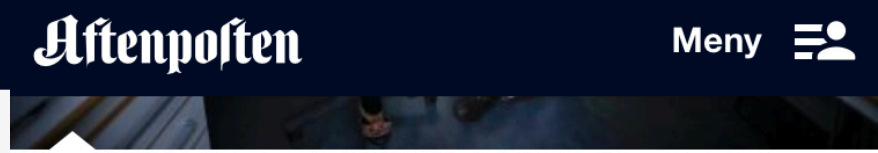


FOTO: Tor Stenersen BILDETEKST

Beskyttelse av pasientsikkerhet er overordnet andre hensyn! | Anne Kjersti Befring

Feiltolkninger av reguleringer av medisinsk behandling og data.

ANNE KJERSTI BEFRING
FORSKER, JURIDISK FAKULTET, UNIVERSITETET I OSLO
PUBLISERT: 08.JAN.2019 14:00
OPPDATERT: 09.JAN.2019 12:49

Flere leger har stilt spørsmål om de må velge å gi pasienter medisinsk behandling med høy risiko for å overholde kravene til databehandling. Det er selvfølgelig en

Aftenposten Meny

Når personvern truer folkehelsen | 32 forskere ved Oslo universitetssykehus

FOTO: Robert McPherson BILDETEKST

Vi har sagt ifra internt i mange år uten at noe har skjedd. Nå finner vi det riktig å gå ut offentlig.

32 FORSKERE VED OSLO UNIVERSITETSSYKEHUS

15 TIMER SIDEN 2 TIMER SIDEN

Aftenposten Meny

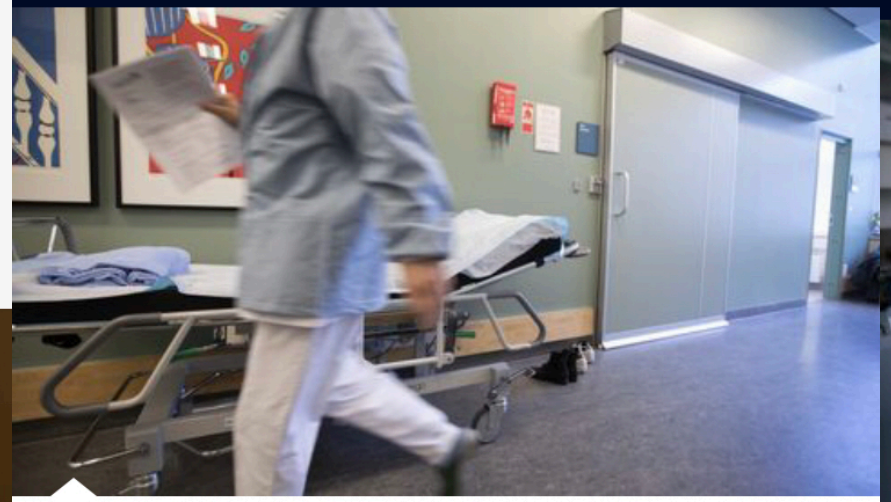


FOTO: Kallestad, Gorm / NTB scanpix

Jeg er rimelig trygg på at pasienter og potensielle fremtidige pasienter alle vil være glade for at vi leger og annet personell lærer av egen praksis.

OLAV RØISE
PROFESSOR VED UNIVERSITETET I OSLO OG LEDER FOR LEGEFORENINGEN FOR KVALITETSFORBEDRING OG PASIENTSIKKERHET

1. JAN. 2019 22:00 2. JAN. 2019 22:07

KRONIKK

Aftenposten Mer

FOTO: Tor Stenersen BILDETEK

– Hvis vi ikke får dele kunnskap, e det god grunn til å snakke om dødelig personvern. Det skriver 3 leger ved Oslo universitetssykehu

JUNE WESTERVELD
TINE DOMMERUD
NINA SELBO TORSET

15 TIMER SIDEN 2 TIMER SIDEN

Medieoppslag

Kravene som oppstilles til databeskyttelse kan kollidere med andre plikter, for eksempel plikter til forsvarlig behandling av pasienter som også er forsøkspersoner.

Aftenposten, jan 2019: Når personvern truer folkehelsen: 32 forskere ved Oslo universitetssykehus

- Praksis: *«Når navn erstattes med en tallkode, fremstår publiserte resultater som anonyme for den som leser artikkelen. Forskningsinstitusjonen har selvsagt en liste der tallkoden er koblet til pasientenes identitet. Det er nødvendig for at man i ettertid skal kunne kontrollere at resultatene er riktige og for å forhindre forskningsjuks.»*
- Tolking av personvernloven *«Fordi det finnes en liste som kobler tallkoder til navn og personnummer, klassifiserer det nye EU regelverket (General Data Protection Regulation, GDPR) resultatene som personopplysninger. De er ikke anonyme, men «avidentifiserte». På OUS leser noen loven ut av kontekst og trekker slutningen at kodede forskningsresultater skal betraktes som så sensitive at de må lagres like sikkert som pasientjournaler og for enhver pris ikke publiseres.»*

Tusen takk for oss

Jurist Grete K Nielsen

Fylkesmannen i Oslo og Viken

23.10.2020