Krav til informasjonssikkerhet

Med utgangspunkt i Normen versjon 5.3 med frempek mot versjon 6.0

Jan Henriksen, sekretariatet for Normen

Innhold

- Informasjonssikkerhet og personvern
- Litt fra personvernforordningen (GDPR)
- Krav til informasjonssikkerhet i Normen 5.3
- Frempek mot Normen versjon 6.0

Informasjonssikkerhet - begrep

- Helsepersonell behandler helse- og personopplysninger om pasient → **Konfidensialitet**
- Helsepersonell – plikt til å føre pasientjournal → **Integritet**
- Forpliktelse ift pasienten – kontinuitet i behandling og omsorg → **Tilgjengelighet**
- Det skal finnes tiltak for å forebygge, detektere, håndtere og gjenopprette personopplysnings-sikkerheten → **Robusthet**

NORMEN

Personvern vs informasjonssikkerhet

Personvern

Rett

- Privatlivets fred
- Regulere bruk av personopplysninger

Informasjonssikkerhet

Plikt

- Virkemidler for å sikre personopplysningene og personvernet
  - Konfidensialitet
  - Integritet
  - Tilgjengelighet
  - Robusthet

Hvorfor en norm?

- Helseopplysninger er ufullstendige
- Uautorisert tilgang og innsyn i helseopplysninger
- Tyveri av utstyr med helseopplysninger
- Tap av lagringsmedia eller bærbar PC med helseopplysninger
- Ødeleggelse av lagringsmedia eller datautstyr

Hvorfor en norm?

- Ny versjon av programvare installeres, men virker ikke – helt eller delvis
- Trådløst nettverk er ikke sikret
- Avtale med leverandør dekker ikke informasjonssikkerhet og personvern
- Velferdstek. samler inn mer data enn besluttet
- Skyløsning skiller ikke behandling av personopplysninger for ulike kunder
- Personvernregler i virksomheten finnes ikke

NORMEN

Pasientombud: Alvorlig at journalsnoking ikke ble fanget opp av sykehusrutiner

Både Datatilsynet og Pasientombudet reagerer på at

Osl

syke

Foreslår nytt straffebud mot deling av krenkende bilder og filmer

Pressemelding | Dato: 26.06.2018
| Nr: 52 – 2018

Justis- og beredskapsdepartementet har i dag sendt på høring et forslag til et nytt straffebud mot deling av krenkende bilder og filmer.

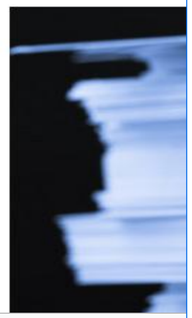
Lege dømt for ulovlig «journalsn

En lege som var ansatt ved Sørlandet sykehus er idømt en bot fra politiet og en advarsel fra Helsetilsynet etter at han ulovlig «snoket» i journaler.

08:1 ga Høyr radiosendinga Tips oss! Klassequizen 2018

Granskar sjukepleiar for snoking i 250 journalar

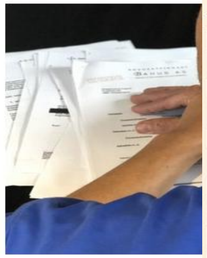
Ein sjukepleiar i ein sunnmørskommune er mistenkt for å ha snoka i 250 pasientjourna
for vide fullma



Saltdal komm
- Imøtekommende, løsningsfokusert og ansvarlig

Pasient får erstatning av «snoke-lege»: – Han har ødelagt livet mitt

Kristiansanderen gikk til søksmål da sykehuset nekta å betale erstatning. I fire måneder visste sykehuset at
inn.



Småbarnsfaren tok opp kampen mot le
FOTO: KARI JEPPESTØL ARNTZEN / NRK

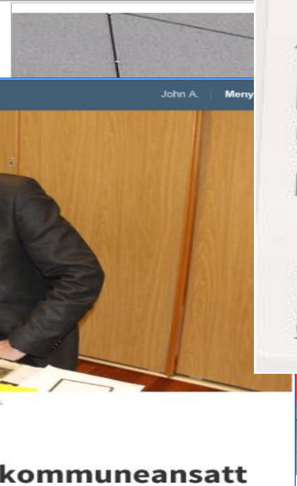
Nabokrangel bidro til at Nav-leder snoket i registre

Loggene fra Nav viser at den tiltalte kvinnen, som var leder i Nav, søkte en rekke ganger på sine nærmeste naboer. Loggen viser 109 oppslag på en nabokvinnen. Hennes ektemann har flere tiltalls oppslag fra Nav-lederen i ulike systemer. Foto: NTB scanpix og faksimile Nav, montasje Nettavisen

En ansatt i Politiet utlendingsenhet e dagers betinget fengsel for å ha snoket i politiets registre.

Oslo tingrett har d
brudd på tjeneste
taushetsplikten, m

Politibetjenten, sc
må i tillegg betale
omfattende snoki
ige stillinger Selvbetje



Fædrelandsvennen Nyheter Sport Kultur God Helg John A. Meny

Rådmann Svein Skisland i Vennesla kommune mener ansatte på jobb ikke skal skal oppleve å bli hengt ut på Facebook.
FOTO: Arkivfoto Odd Inge Ulleberg

LOKALT

Anmelder person som filmet kommuneansatt

Rådmann Svein Skisland i Vennesla har anmeldt en privatperson for å poste film av en kommuneansatt i tjeneste på Facebook.

Advarsel til Saltdals befolkning- Phising = digital snoking

Tiden nærmer seg at folk forventer å høre hvordan «det gikk på skatten».
I denne sammenheng vil svindlere sende ut mailer der du får beskjed å om følge en link for å se hvor mye penger du har fått igjen.
Dette kalles på dataspråk for Phising.
Vær derfor forsiktig med hva dere trykker på. Hvis dere har mistanke om at dette er forsøk på svindel, så ikke trykk på lenkene og ikke gi fra dere personlige opplysninger. Den falske siden er veldig lik den reelle siden fra Skatteetaten.

sikerer sparken etter snoking

åværende og tidligere ledere har snoket i sensitive personopplysninger om kolleger i etaten.

Hertz BilPool

Frihet på deling

Hei,

Du mottar denne informasjonen fordi du er medlem av Hertz BilPool og er berørt av et sikkerhetsbrudd hos oss.

Vi verdsetter din integritet og respekterer personvernet og dine personlige opplysninger. Vi ønsker derfor proaktivt å gi deg skriftlig beskjed om en datasikkerhetshendelse som kan knytte seg til dine personlige data.

Hva har skjedd?
Den 18. april ble Hertz BilPool oppmerksom på at det var en mulighet for at personopplysninger fra enkelte kunder kunne åpnes på en uautorisert måte. De tilgjengelige personopplysningene var bilder av førerkort fra vår database. Vi vil understreke at det *kun var bildet* som ligger i din profil som var tilgjengelig. Ingen annen data eller informasjon fra din profil var tilgjengelig

Behandling av personopplysninger (art 9)

”«behandling» enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring”

NORMEN

Personopplysninger (art 4)

”enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet”

NORMEN

Særlig kategorier personopplysninger (art 9)

”Opplysninger om

a) rasemessig eller etnisk opprinnelse
b) politisk oppfatning
c) religion
d) filosofisk overbevisning
e) fagforeningsmedlemskap
f) genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person
g) helseopplysninger
h) opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering”

Hva med 11-siffret fødselsnummer?

NORMEN

Databehandler

- Med databehandler menes den som behandler helse- og personopplysninger på vegne av den dataansvarlige
- En databehandler er en ekstern person eller virksomhet utenfor den dataansvarliges virksomhet
- Eksempel: leverandør drifter samhandlingsportal for oppvekst

Mal for databehandleravtale finnes på normen.no

NORMEN

Krav til informasjonssikkerhet

- Ansatte, kompetanse og holdningsskapende arbeid
- Tilgangsstyring
- Fysisk sikkerhet og håndtering av utstyr
- Sikker IT-drift / Teknisk sikkerhetsløsning
- Digital kommunikasjon med pasienter/bruker
- Leverandørforhold og avtaler
- Håndtering av informasjonssikkerhetsbrudd
- IKT-beredskap

For å oppfylle kravene til konfidensialitet, integritet, tilgjengelighet og robusthet

NORMEN

Tilgangsstyring

- All tilgang til helse- og personopplysninger skal baseres på tildelt autorisasjon i fagsystemet og tjenstlig behov – rolle kan benyttes
- Autorisasjon for å
  - lese, registrere, redigere, skrive ut, rette, slette og sperre helse- og personopplysninger
- Fellesbruker er ikke tillatt
- All tildeling av autorisasjon skal registreres i et autorisasjonsregister
- Alle tildelte autorisasjoner skal kontrolleres minimum årlig

NORMEN

Tilgang for teknisk personell

- Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for større mengder helse- og personopplysninger
- Det skal iverksettes tiltak slik at mulig misbruk av teknisk personell skal kunne avdekkes
  - Tilgang gis via en personlig administratorkonto
  - Engangspassord
  - Sterk autentisering (sikkerhetsnivå 3 eller 4)
  - Logging
  - …

NORMEN

Autentisering

- Autentisering skal:
  - sikre identifisering av den enkelte bruker
  - sikre identifisering i korrekt rolle (om rolle benyttes)
  - ved behov kreve ulike autentiseringskriteria for hver rolle (om rolle benyttes)
- Ulike ansettelsesforhold skal identifiseres
- Autentiseringen skal være tilstrekkelig ift risikovurdering

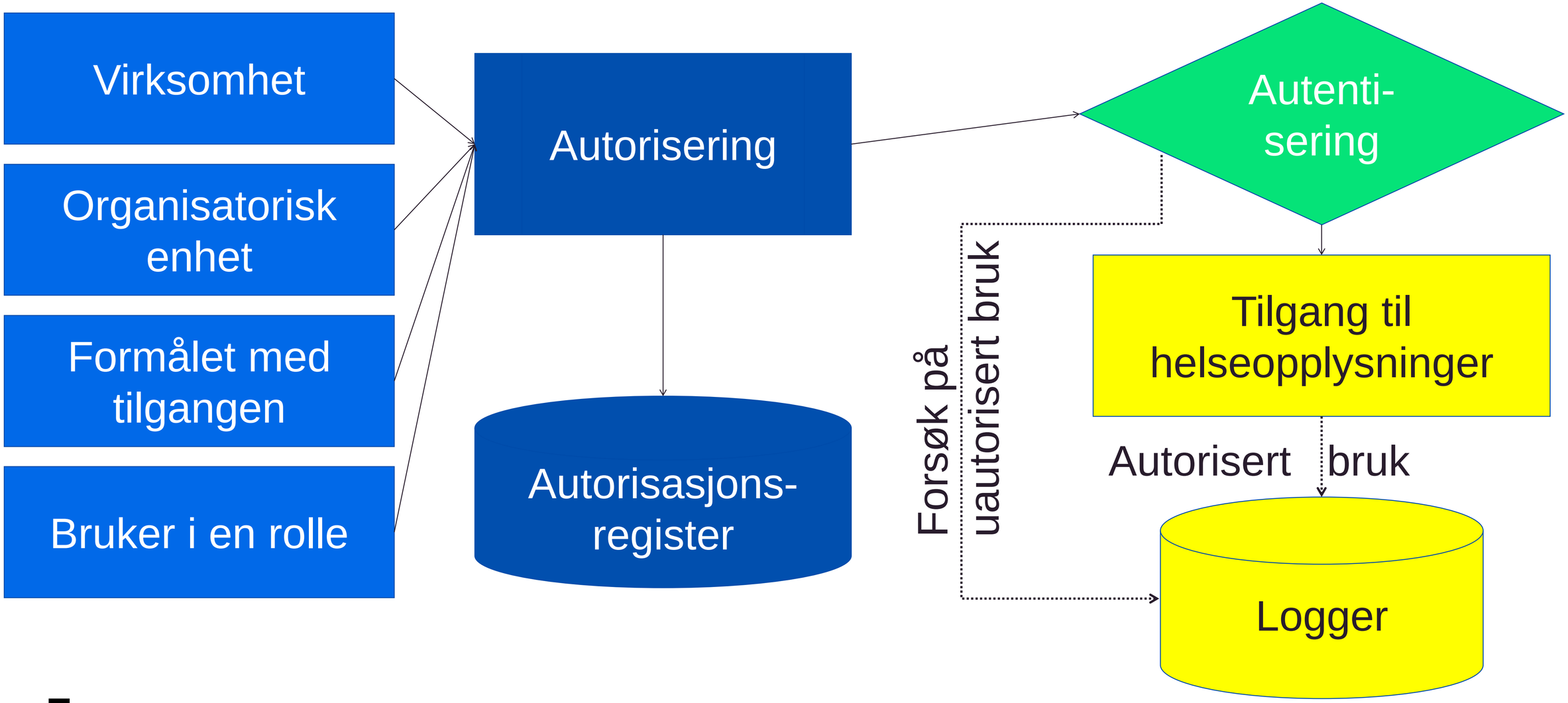
NORMEN

Autorisasjonsregister

- Dataansvarlig skal sørge for at det opprettes et autorisasjonsregister
- Registeret skal som minimum inneholde:
  - informasjon om hvem som er tildelt autorisasjon
  - til hvilken rolle autorisasjonen er tildelt (om rolle benyttes)
  - formålet med autorisasjonen
  - tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt
  - informasjon om hvilken virksomhet den autoriserte er knyttet til
- Hver oppføring skal arkiveres i 5 år
  - fra det tidspunkt autorisasjonen tas ut av bruk

NORMEN

Tilgangsstyring



NORMEN

Kontroll av tilgangsrettigheter

- Jevnlig kontroll av hvem som har hatt tilgang
- Kontroll skal utføres
  - Ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde.
  - Minimum årlig (gjerne i forbindelse med sikkerhetsrevisjon).
  - Ved sikkerhetsbrudd for det informasjonsområdet som blir berørt av bruddet
- Varsling
  - Til ledelsen ved mistanke om urettmessig tilgang
  - Til Datatilsynet ved faktisk hendelse

NORMEN

Tilgang mellom virksomheter

PJL § 19

PJL § 9

- Reservasjonsrett
- Tilgangsstyring – kun relevante og nødvendige opplysninger ift ytelsen av helsehjelp
- Sikker autentisering
- Logging ut over ordinær logging
- Aktiv kontroll av benyttede tilganger

Med ”sikker autentiseringsløsning” menes i Normen en autentiseringsløsning som for eksempel er basert på personlig kvalifisert sertifikat eller annen autentiseringsløsning som gjennom en risikovurdering viser at den har tilstrekkelig sikkerhet

NORMEN

Fysisk sikring

- Server og kommunikasjonsutstyr skal være i bemannet eller avlåst område
- Sikring av PC
  - Kryptering av lagringsenhet på bærbart utstyr
- Soneprinsipp ifm. resepsjoner, datarom, behandlingsrom, mv.
- Faktaark 17 – Fysisk sikring av områder og utstyr

NORMEN

Plassering av utstyr

- Plasser skjerm og skriver skjermet for innsyn og adgang
  - Taushetsplikten – den passive delen
- Skjermsparer m/passord
  - Taushetsplikten – den passive delen

NORMEN

Sikker IT-drift

- Konfigurasjonskontroll
- Driftsrutiner (jf. styringssystemet)
- To uavhengige tekniske tiltak mot eksterne nettverk
  - Skille behandling av helseopplysninger og eksterne nettverk
- Teknisk løsning med sikkerhetsbarrierer
  - Hindre uautorisert tilgang / kun eksplisitt trafikk
  - Antivirus / ødeleggende programvare
  - All kommunikasjon skal starte innenfra eget nettverk

NORMEN

Sikkerhets- og tilbakekopiering

- Dokumenterte rutiner
  - Frekvens
  - Ansvar
- Sikkerhetskopi skal oppbevares
  - Avlåst
  - Brannsikkert
  - Adskilt fra driftsutstyret (server)
- Jevnlig teste at sikkerhetskopiene
  - er korrekte
  - kan tilbakeføres

NORMEN


JEG GLEMTE IKKE IGJEN BACKUP-DISKENE HER?
SLANE
ca.nz

Logging

- Autorisert bruk
- Forsøk på uautorisert bruk
- Logger (autorisert bruk av fagsystemet) skal minimum inneholde
  - Identitet til den som har hentet fram helseopplysninger
  - rollen den autoriserte brukeren har ved tilgangen
  - virksomhetstilhørighet
  - organisatorisk tilhørighet til den som har hentet fram helseopplysninger
  - hvilke type opplysninger det er gitt tilgang til
  - hvem som har fått utelevert helseopplysninger
  - grunnlaget for tilgjengeliggjøringen
  - tidsperioden for tilgjengeliggjøringen

NORMEN

Logging

- For forsøk på uautorisert bruk
  - brukeridentiteten som ble benyttet
  - tidspunkt (dato og klokkeslett)
  - IP-adresse eller annen identifikasjon av PC/arbeidsstasjon som ble benyttet (for eksempel MAC-adresse eller NAT-adresse)
- Logger skal oppbevares til det av helsehjelpens karakter ikke lenger antas å bli bruk for dem
- Logger skal analyseres (ukentlig)

NORMEN

Den registrertes rettigheter

- Skal ha informasjon om rettigheter
- Innhente samtykke når det er nødvendig
- Ivareta de faktiske rettighetene til innsyn i, redigering, sletting og sperring (reservasjonsrett) av registrerte opplysninger om seg selv
- Innsyn i logger

NORMEN

…, jeg trodde jeg hadde innsynsrett..

NORMEN

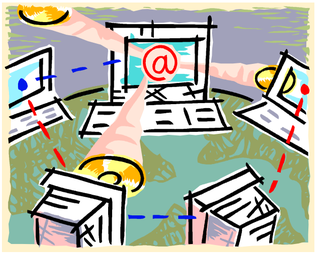
Innsyn i logger

- Pasientjournal og logger ”er ett”
- Innsyn iht dokumentert rutine
- Minimum informasjon om:
  - Person og organisatorisk tilhørighet til den som har behandlet helseopplysningene
  - Hvilke behandlinger som er utført
  - Når behandlingene er gjort

NORMEN

Teknisk sikkerhetsløsning

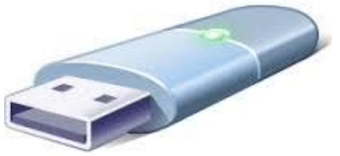
- Kryptering av ekstern kommunikasjon
  - Oppfylle krav fastsatt av NSM
- Autentisering som for stasjonært utstyr gjelder for
  - mobilt utstyr
  - hjemmekontor / fjernaksess fra leverandør
  - trådløs kommunikasjon
  - linjer virksomheten ikke har fysisk kontroll over



Tekniske sikkerhetsløsninger

- ”Skytjenester” (fjernlagring, synkronisering, kontorstøtte, osv)
  - Risikovurdering av behandling av helse- og personopplysninger
  - Databehandleravtale – norsk rett gjelder
  - Virksomheten og databehandler har ansvaret

Flyttbare medier



- Merkes tydelig
- Skal krypteres
- Slettes forsvarlig - destrueres ved utrangering
- Oppbevares avlåst
- Sendes som rekommandert post (anbefaling i faktaark)

NORMEN

Service / utrangering av utstyr

- Fjernes utstyr som inneholder helse- og personopplysninger fra virksomheten, må det opprettes en databehandleravtale med serviceyter
  - Service på stedet er å anbefale, men ikke et krav
- Ved utrangering av utstyr/lagringsmedia skal lagringsmedia slettes forsvarlig eller destrueres (for eksempel skriver)

NORMEN

Digital samhandling – ordinær SMS og e-post

- Skal aldri brukes til helseopplysinger
- Skal aldri inneholde 11-sifferet fødselsnummer (art 5, nr 1. f) + 32)
- Mottas helseopplysninger via SMS eller e-post svarer virksomheten at ”Henvendelser med helseopplysninger blir ikke besvart. Bruk telefon eller fremmøte”
- Veileder: Portalløsninger, SMS og e-post

NORMEN

Utskrifter / faks (papirdokumenter)

- Rutiner for behandling av utskrifter (K)
  - Sikring
  - Arkivering
  - Makulering
- Bruk av faks for helse- og personopplysninger (K)
  - Anonymiseres
  - Samtykke fra pasienten

NORMEN

Håndtering av informasjonssikkerh

- Rutine
- Faktainnsamling og vurderin
- Tiltak
- Melding til Datatilsynet innen 72 timer
  - Hva skal meldes?
- Melding til den registrerte - hvilke unntak skal det tas hensyn til?
  - Det er gjennomført tekniske og organisatoriske sikkerhetstiltak
  - Det er truffet tiltaket i etterkant
  - Om varslingen innebærer en uforholdsmessig stor innsats

Utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-utorisert tilgjengeliggjøring av eller tilgang

NORMEN

Hjemmekontor

- Tekniske tiltak slik at det kun kan kommuniseres med predefinert utstyr
- Autentisering som for stasjonært utstyr
- Utskrift er ikke å anbefale
  - Hvis utskrift; sikring, arkivering, makulering
- All kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer sikres ved kryptering
- Kryptering av lagringsenhet

NORMEN

Andre krav i Normen

- Taushetsplikten – aktiv og passiv
- Nødrutiner skal utarbeides – hva gjør virksomheten om alle journaler er borte eller ikke tilgjengelige?
- Avtaler
- Kontroll av tilgangsstyring ved sikkerhetsbrudd
- All bruk av selvautorisering skal grunngis og følges opp som avvik
- …

NORMEN

Taushetsplikten i hverdagen

- Passiv plikt
  - Hvem snakker du med
  - Hvem lytter
  - Hvem utleveres opplysninger til

- Aktiv plikt
  - Skjermsparer med passord – manuell / automatisk
  - Plassering av utstyr
  - Låse kontor
  - Låse ned dokumenter og notater
  - Makulere
  - Reelle data som testdata
  - Utrangering av teknisk utstyr (multifunksjonskriver)
  - …

NORMEN

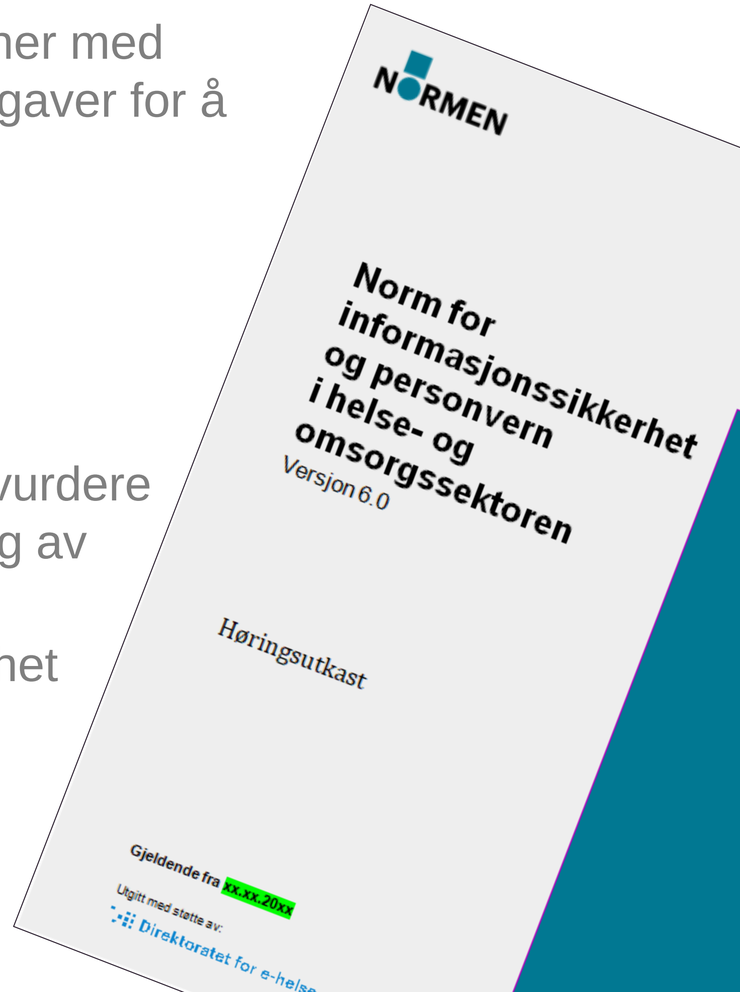
Oppsummering

- Informasjonssikkerhet og personvern
- Litt fra personvernforordningen (GDPR)
- Krav til informasjonssikkerhet i Normen 5.3
- Frempek mot Normen versjon 6.0

NORMEN

Frempek mot Normen 6.0

- Roller og ansvar for informasjonssikkerhet og personvern
  - Virksomhetens øverste ledelse skal sørge for å etablere roller og funksjoner med tilstrekkelige ressurser og kompetanse til å gjennomføre nødvendige oppgaver for å ivareta ansvaret.
- Dataansvarliges ansvar
- Databehandlers ansvar
- Forholdsmessighet ved valg av tiltak
  - Ved valg av egnede tekniske og organisatoriske tiltak skal virksomheten vurdere tiltakene i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv.
- Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet



NORMEN

Frempek mot Normen 6.0

- Grunnleggende om behandling av helse- og personopplysninger
- Leverandører skal tilrettelegge for at dataansvarlig som tar i bruk leverandørens produkter og tjenester, kan oppfylle lovbestemte krav og krav i Normen
- Tilintetgjøring av dokumenter mv. etter digitalisering
- Pasientjournaler ved opphør av virksomhet mv.
- Tilgangsstyring
- Skjerping av administratorbruker (personlig, separat konto, ulike administratorbrukere til ulike deler av infrastrukturen)
- Tidsbegrensning i autorisasjon
- Sikker autentisering (tilgang til helseopplysninger, hjemmekontor, mobilt utstyr, trådløst nettverk)
- Endre standardpassord

Frempek mot Normen 6.0

- Kryptering iht. «NSM Cryptographic Requirements Version 3.1» og Level Moderate
- Dataansvarlig eller databehandler/tjenesteleverandør skal etablere og vedlikeholde en helhetlig sikkerhetsarkitektur som gir en sikker og forsvarbar infrastruktur som gjenspeiler nivå for akseptabel risiko
- Dokumentere dataflyt, datakommunikasjon og integrasjoner
- Kun godkjent utstyr og programvare skal benyttes til behandling av helse- og personopplysninger
- Maskin- og programvare skal oppdateres slik at den nyeste og mest tidsaktuelle sikkerhetsfunksjonaliteten følger med og nødvendige sikringstiltak benyttes
- Det skal benyttes separate miljøer for utvikling, test og produksjon
- Konfigurasjonen av utstyr og programvare skal jevnlig sjekkes slik at den kun utfører formålsbestemte funksjoner.
- Konfigurasjonen skal beskyttes mot ondsinnet programvare

Frempek mot Normen 6.0

- Minimum en sikkerhetskopi skal beskyttes mot ondsinnet programvare
- Logging av
  - all system- og administratorbruk til informasjonssystemer og infrastrukturen
  - endring av konfigurasjon og programvare
- Minimum innhold i logger
- Teknisk utstyr eller applikasjoner som kobles til internett, skal inkluderes i virksomhetens arbeid med informasjonssikkerhet og personvern, herunder i risikovurderinger, tilgangsstyring og rutiner for bruk
- …må journalsystemer og fagsystemer ha funksjonalitet som oppfyller relevante krav i Normen
- Skytjenester
- Nødrutinene skal øves på, testes, revideres og oppdateres minst en gang i året

NORMEN