Krav til informasjonssikkerhet

Normen versjon 6.0 – Kapittel 5. Informasjonssikkerhet

Jan Henriksen

sekretariatet for Normen

Innhold

- Informasjonssikkerhet og personvern
- Litt fra personvernforordningen (GDPR)
- Krav til informasjonssikkerhet i Normen

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 / rettigheter

Informasjonssikkerhet

Plikt

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

NORMEN

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

Sikre god helsehjelp

NORMEN

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

- Velferdsteknologi samler inn mer data enn besluttet
- Skyløsning skiller ikke behandling av personopplysninger for ulike kunder
- Personvernregler finnes ikke i virksomheten

NORMEN

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”

IP-adresse, GPS-koordinator

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

MTU og Normen

- *”Medisinsk utstyr som behandler helse- og personopplysninger, skal inkluderes i virksomhetens arbeid med informasjonssikkerhet og personvern, herunder i risikovurderinger, tilgangsstyring, endringskontroll og rutiner for bruk, på linje med andre informasjonssystemer*”
- Tilsvarende formulering i kap 5.5.5 Tilkobling til Internett

NORMEN

Kap 5 - Krav til informasjonssikkerhet

1. Ansatte, kompetanse og holdningsskapende arbeid
2. Tilgangsstyring
3. Fysisk sikkerhet og håndtering av utstyr
4. Sikker IT-drift
5. Kommunikasjonssikkerhet
6. Digital kommunikasjon til den registrerte
7. Leverandørforhold og avtaler
8. Håndtering av informasjonssikkerhetsbrudd
9. Nødrutiner

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

NORMEN

2. Tilgangsstyring

- All tilgang skal baseres på tildelt autorisasjon i fagsystemet og tjenstlig behov
- Autorisasjon skal skille rettigheter for å lese, registrere, redigere, rette, slette og sperre helse- og personopplysninger
- Autorisasjon skal være tidsbegrenset
- Fellesbruker er ikke tillatt
- All tildeling av autorisasjon skal registreres i et autorisasjonsregister

NORMEN

Tilgang for teknisk personell

- Tilgangsstyring skal etableres for administrator- og systembrukere
- Bruker med administratortilganger skal benytte personlig separat brukerkonto for administratoroppgaver
- Driftspersonell skal ha personlige brukerkontoer for oppgaver som ikke krever administratortilganger
- Det skal etableres tiltak slik at mulig misbruk skal kunne avdekkes
  - For eksempel sterk autentisering, logging

NORMEN

Autorisasjonsregister

- Virksomheten skal opprette et autorisasjonsregister
- Registeret skal som minimum inneholde:
  - hvem som er tildelt autorisasjon
  - til hvilken rolle autorisasjonen er tildelt (om rollen benyttes i virksomheten)
  - formålet med autorisasjonen
  - tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt
  - informasjon om hvilken virksomhet den autoriserte er knyttet til
  - helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet (kun om tilgang til helseopplysninger i annen virksomhet er tatt i bruk)

NORMEN

Tilgang mellom virksomheter

PJL § 19

- Det skal gjennomføres risikovurdering ved oppstart eller endring av tilgjengeliggjøring av opplysninger for andre virksomheter
- Reservasjonsretten skal ivaretas
- Sikker autentisering (for eksempel ”Betydelig” eller ”Høyt” - Nkom)
- Logging av tilgang
- 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

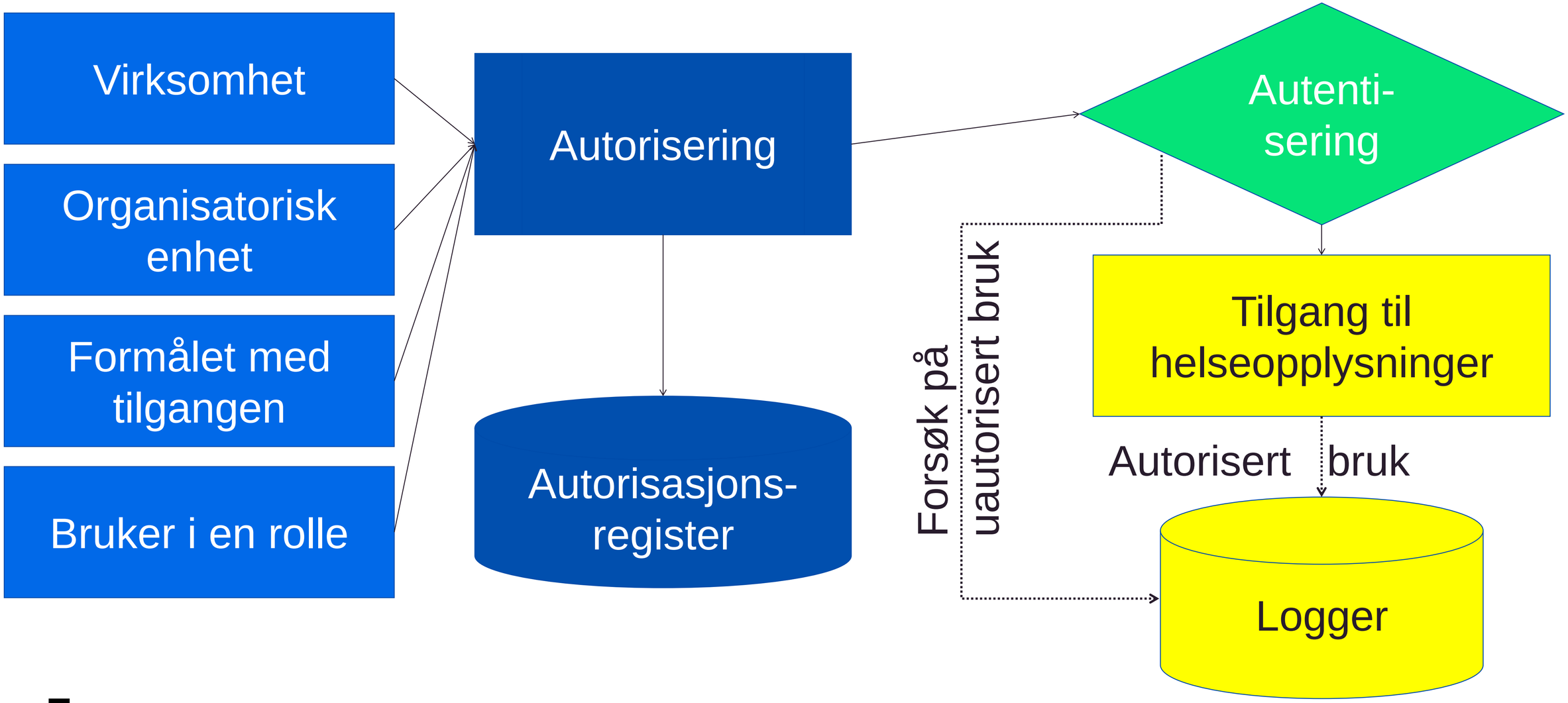
NORMEN

Autentisering

- Den autoriserte skal bekrefte sin identitet på en sikker måte
  - Sikker måte må besluttes på grunnlag av en risikovurdering
- Ulike ansettelsesforhold skal identifiseres
- Flere personer skal ikke benytte samme autentiseringskriterier
- Alle standardpassord (fabrikkinnstillinger) på systemer og utstyr skal endres
- Ved bruk av trådløse nettverk skal den autoriserte brukeren autentiseres med sikker autentiseringsløsning

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 som blir berørt av bruddet
- Varsling til ledelsen ved mistanke om urettmessig tilgang
- Misbruk av selvautorisering skal følges opp som avvik
- Dersom kontrollen viser at det har skjedd en urettmessig tilgang, skal dette behandles som et avvik

NORMEN

3. Fysisk sikring og håndtering av utstyr

- Hindre at uautoriserte får tilgang til helse- og personopplysninger
- Hindre at uautoriserte får adgang til infrastruktur
- Helseopplysninger skal lagres kryptert ved lokal lagring
- Kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll skal krypteres
  - Kryptering og dekryptering mellom kommunikasjonspunkter i infrastrukturen skal gjøres i godkjent utstyr virksomheten har kontroll med
  - Kontrollen kan ivaretas gjennom avtale

NORMEN

4. Sikker IT-drift

- Konfigurasjonskontroll
  - Utstyr og programvare skal kun utfører de funksjonene som er formålsbestemt
  - All dataflyt, datakommunikasjon og integrasjoner skal kartlegges og dokumenteres
  - Kun godkjent utstyr og programvare skal benyttes
  - Maskin- og programvare skal oppdateres (patches)
    - Verifisering og testing skal dokumenteres
  - Planlagte endringer skal følge rutine for konfigurasjonsendringer.
  - 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
  - Konfigurasjonen skal beskyttes mot utilsiktede handlinger

NORMEN

Konfigurasjonskontroll

- Konfigurasjonsendringer, skal ikke settes i drift før følgende tiltak er gjennomført:
  - Risikovurdering som viser at nivå for akseptabel risiko oppfylles
  - Test som sikrer at forventede funksjoner er ivaretatt
  - Implementering som sikrer mot uforutsette hendelser
  - Ny konfigurasjon er dokumentert
  - Konfigurasjonsendringer er godkjent av virksomhetens leder eller den ledelsen bemyndiger
- Konfigurasjonskontroll skal reguleres gjennom avtale ved
  - bruk av databehandler
  - bruk av fjernaksess for vedlikehold og oppdateringer

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

Sikkerhetskopiering

- Dokumenterte rutiner
  - Frekvens
  - Ansvar
- Sikkerhetskopi skal oppbevares
  - Avlåst
  - Brannsikkert
  - adskilt fra driftsutstyret (server)
- Jevnlig teste at sikkerhetskopiene
  - er korrekte
  - kan tilbakeføres
- Minimum en sikkerhetskopi skal beskyttes mot ondsinnet programvare og uønskede hendelser

NORMEN


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

Logging

- For å oppdage brudd eller forsøk på brudd skal det som minimum logges:
  - Autorisert bruk av informasjonssystemene
  - All system- og administratorbruk til informasjonssystemer og infrastrukturen
  - Endring av konfigurasjon og programvare
  - Sikkerhetsrelevante hendelser i sikkerhetsbarrierer
  - Forsøk på uautorisert bruk av informasjonssystemer og infrastrukturen
  - Bruk av selvautorisering

Logging

- Følgende skal som minimum registreres i loggene ved autorisert bruk av behandlingsrettet helseregister:
  - Identiteten til den som har lest, rettet, registrert, endret og/eller slettet opplysninger
  - Organisatorisk tilhørighet
  - Grunnlaget for tilgjengeliggjøringen
  - Tidsperioden for tilgjengeliggjøringen
- Loggene skal enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd
- Det skal etableres rutiner for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser – proaktiv analyse av logger
  - Dersom brudd avdekkes, skal dette håndteres som et avvik

Logging

- Det skal etableres rutiner for ved behov å kunne sammenholde loggene med autorisasjonsregister
- Loggene og autorisasjonsregister skal sikres mot endring og sletting
- Logger skal ha korrekt tidsstempel
- Logger som genereres ved ytelse av helsehjelp, skal lagres til det ikke antas å være bruk for dem
- Logger av sikkerhetsmessig betydning bør oppbevares så lenge som nødvendig for å oppnå formålet

NORMEN

Logging

- Forsøk på uautorisert bruk – eksempel på innhold
  - 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)

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

…, jeg trodde jeg hadde innsynsrett..

NORMEN

Sikkerhetsrevisjon

- Virksomhetens ledelse skal følge opp at sikkerheten ivaretas ved jevnlige og minimum årlige sikkerhetsrevisjoner
  - ➢kontrollere og kvalitetssikre etablerte tiltak og fastsatte rutiner
- Det skal foreligge en godkjent plan for sikkerhetsrevisjoner
- Resultatene, konklusjonene og avvik fra sikkerhetsrevisjonene skal dokumenteres og håndteres av virksomheten

~~FA 6b og 38~~

Samlet oversikt Normens krav

Nr	Krav (formulert som spørsmål)	Kap. i Normen	Kap. i ISO 27001 og Annex A	Systemkrav i behandlings-rettet helse-register	Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes)	Er kravet ivaretatt?	Hjemmel til kravet i lov eller forskrift	Kravet blir ivaretatt av data-behandler
1.	Er valg av egnede tekniske og organisatoriske tiltak vurdert i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv?	1.5	6.1.1 8.1			☐Ja ☐Nei	PVF artikkel 32 PJL § 22 HRL § 21 FLK § 6	
2.	Er valgte tiltak basert på risikovurderinger?	1.5	6.1.3 8.3			☐Ja ☐Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	☐Ja ☐Nei
3.	Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger?	1.5	6.1* 8.1.*			☐Ja ☐Nei	PVF artikkel 32 PVF artikkel 35 (1) PJL § 22 HRL § 21	
4.	Sørger virksomhetens øverste leder for virksomheten at gjeldende krav til informasjonssikkerhet og personvern følges?	2	5.1 5.2 5.3			☐Ja ☐Nei	PJL § 22 HRL § 21 HTL § 5-10 første punktum PVF artikkel 24 FLK § 7	
5.	Har virksomhetens øverste leder bestemt nivå for akseptabel						PJL § 22	

NORMEN

5. Kommunikasjonssikkerhet

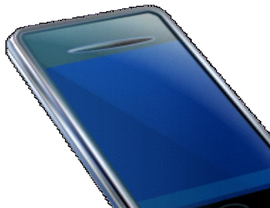
- Krav for nettverkssikkerheten skal defineres og dokumenteres
  - Tiltakene skal være basert på risikovurdering
- Ved tilkobling til eksterne nett skal tiltak sikre at eksplisitt angitt tillatt trafikk kan passere utenfra og inn eller motsatt, og at annen trafikk stoppes
  - Det skal være minst to uavhengige tekniske tiltak slik at personer utenfor virksomheten ikke skal kunne få uautorisert tilgang, endre eller slette opplysninger
- Det skal avtales klare ansvarsforhold mellom avsender, mottaker og eventuell meldingsformidler
  - Alle avtaler skal være skriftlige

NORMEN

SMS og e-post

- Ved bruk av ukrypterte kanaler, skal virksomheten
  - forsikre seg om at e-post ikke inneholder identifiserbare helseopplysninger
  - etablere logging for å kontrollere at regler ikke brytes
    - Regelbrudd skal håndteres som avvik, og personalmessige konsekvenser skal vurderes.
  - vurdere om den samlede informasjonen i SMS og e-post kan medføre brudd på taushetsplikten

- Skal aldri brukes til helseopplysinger
- Skal aldri inneholde 11-sifferet fødselsnummer (art 5, nr 1. f) + art 32)
- Veiledning; 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

6. Digital kommunikasjon til den registrerte

- Virksomheten skal
  - beslutte behandlingsgrunnlag
  - vurdere egnet løsning og kommunikasjonskanal
  - sørge for at pasient ikke er avhengig av å lagre opplysningene på eget utstyr for å gjøre seg kjent med informasjonen
  - gjennomføre tilstrekkelige tiltak for å sikre at meldinger sendes til rett mottaker
    - For å sikre korrekt kontaktinformasjon til mottager bør virksomheter som har tilgang til kontakt- og reservasjonsregisteret (KRR), benytte dette

7. Leverandørforhold og avtaler

- Databehandler - ”den som behandler personopplysninger på vegne av dataansvarlig”
  - Eksempel: leverandør drifter EPJ eller backupløsning
- Dataansvarlige kan bare bruke databehandlere som oppfyller kravene i Normen
- Databehandler
  - skal bare behandle helse- og personopplysninger etter instruks fra dataansvarlig
  - skal ikke bruke underleverandør uten tillatelse fra dataansvarlig
  - er ansvarlig for at sine underleverandører
  - skal føre en oversikt (protokoll) over behandlingsaktiviteter
  - skal ved hjelp av tekniske tiltak etablere skiller mellom virksomhetene

NORMEN

Mal for databehandleravtale finnes på normen.no

Vedlikehold, fjernaksess eller fysisk service

- Leverandørens utstyr
  - skal ikke ha ondsinnet programvare
  - skal være sikret mot adgang fra uvedkommende
- All tilgang og fysisk adgang skal være autorisert av virksomheten
  - Tilgangen skal logges og adgangen skal kontrolleres
- Tilgjengelighet til helse- og personopplysninger skal opprettholdes når leverandøren utfører arbeid på utstyr/programvare

NORMEN

Systemleverandører

- Informasjonssystemene skal ha funksjonalitet som oppfyller lovbestemte krav og relevante krav i Normen
- Informasjonssikkerhet og personvern knyttet til anskaffelser og leverandøroppfølging skal inngå i styringssystem for informasjonssikkerhet
  - Alle faser i leverandørstyring, fra anskaffelse til avtalen er avsluttet, skal omfattes
- Virksomheten skal
  - stille krav om innebygd personvern
  - sikre at relevante sikkerhetskrav inngår i alle anskaffelser
  - sørge for at den har tilstrekkelig bestillerkompetanse tilgjengelig

NORMEN

Skytjenester

- Applikasjonsdrift, fjernlagring, synkronisering, kontorstøtte, osv
  - Risikovurdering av behandling av helse- og personopplysninger
  - Databehandleravtale – norsk rett gjelder
  - Hvor lagres helse- og personopplysninger
  - Virksomheten og databehandler har ansvaret

Ny versjon kommer

NORMEN

8. Håndtering av informasjonssikk

- Rutine for avviksbehandlin
- Faktainnsamling og vurderin
- Tiltak
- Melding til Datatilsynet innen 72 timer
  - Krav til innhold i melding
- Melding til den registrerte - unntak finnes
  - 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

Varsel til Statens helsetilsyn

- Varsle om avvik som følge av feil og avvik på informasjonssystemer
- Varslingsplikten utløses
  - ved dødsfall eller svært alvorlig skade på pasient eller bruker
  - som følge av ytelse av helse- og omsorgstjenester
  - når utfallet er uventet ut fra påregnelig risiko
- Ved slike hendelser skal virksomheten
  - følge opp og informere pasienter og pårørende
  - gjennomgå hendelsen
  - identifisere og følge opp risikoreduserende tiltak

NORMEN

HELSETILSYNET
tilsyn med barnevern, sosial- og helsetjenestene

9. Nødrutiner

- Nødvendige helse- og personopplysninger skal være tilgjengelige
- Konsekvenser av bortfall skal kartlegges
- Systemer skal klassifiseres
  - Inklusive hvilke andre systemer og hvilken infrastruktur de klassifiserte systemene er avhengige av
- Virksomheten skal etablere nødrutiner:
  - Alternativ drift uten bruk av informasjonssystemene
  - Alternativ drift med delvis støtte fra informasjonssystemene
- Nødrutinene skal øves på, testes, revideres og oppdateres minst en gang i året

Litt om den registrertes rettigheter

- Skal ha informasjon om rettigheter
- Innhente samtykke når det er nødvendig
- Reservasjonsretten skal ivaretas
- Rettigheter til innsyn, retting, sletting og sperring av registrerte opplysninger om seg selv
- Innsyn i logger

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

NORMEN

NORMEN