Tema	Klokkeslett
Intro om kurset	09:00
Om Normen	09:15
Spørsmål	*09:35*
Pause	09:45
Risikovurdering/ styring	10:00
Pause	10:45
Internkontroll	10.55
Utvalgt temaer om personvern	11:25
Spørsmål	11:45
Lunsj	12.00
Utvalg av Normens krav til informasjonssikkerhet, kap. 5	12:45
Spørsmål	13:30
Pause	13:45
Normens krav i anskaffelser	14:00
Normens handlingsplan 2021 og veiledningsmateriell	14:30
Spørsmål	14:50
Takk for i dag	15:00

NORMEN

Normen 6.0 og krav til informasjonssikkerhet

Introkurs Normen

Informasjonssikkerhet

Tilgjengelighet

Helse- og personopplysninger er tilgjengelig til den tid og på det sted det er behov for opplysningene.

Tilgjengelig informasjon for helsepersonell er en forutsetning for god og forsvarlig behandling

Konfidensialitet

Helse- og personopplysninger må være sikret mot at uvedkommende får kjennskap til opplysningene.

Ivaretakelse av taushetsplikt og personvern er viktig for innbyggernes tillit til helse- og omsorgstjenesten

Integritet

Helse- og personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting.

Korrekt og oppdatert informasjon er en forutsetning for god kvalitet i pasientbehandlingen.

Kapittel 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

5.1 Ansatte, kompetanse og holdningsskapende arbeid

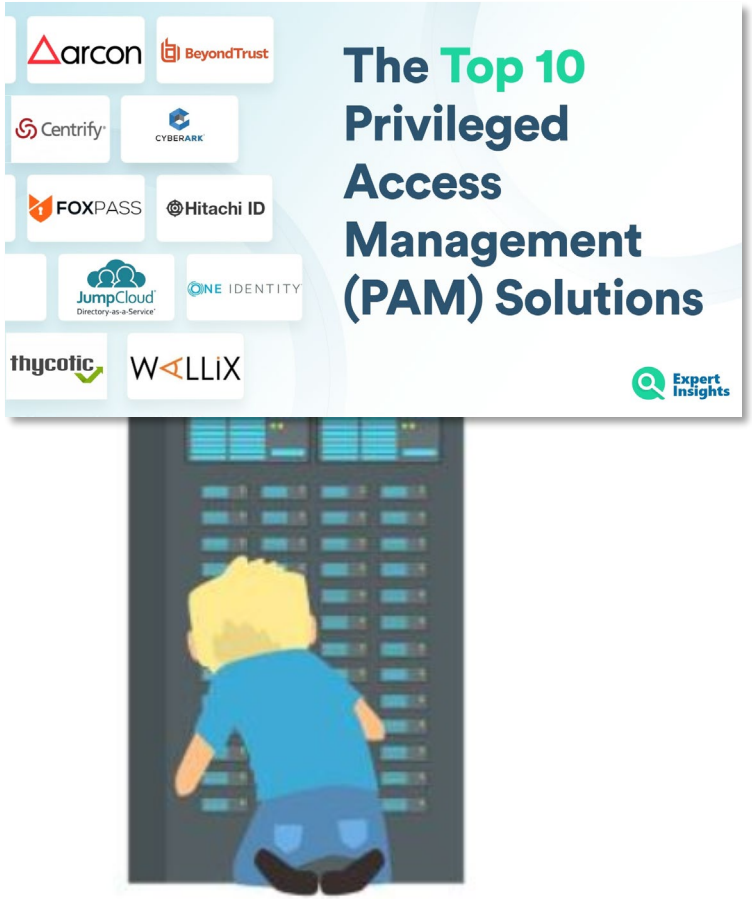
- Kontinuerlig opplæring i taushetsplikt, informasjonssikkerhet og personvern
  - Bør følges opp og dokumenteres
- Taushetserklæring
- Instruks for privat bruk av informasjonssystemer og utstyr
- Opphør av arbeidsforhold
  - Tilbakelevering av ansattkort og medier
  - Sperre tilganger
  - Rutiner for opprydding i informasjon brukeren kan ha lagret

5.2 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** for tilgang til helse- og personopplysninger er **ikke tillatt**
- All tildeling av autorisasjon skal registreres i et **autorisasjonsregister**

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, kontroller



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

Autentisering

- Den autoriserte skal bekrefte sin identitet på en sikker måte
  - Sikker måte må besluttes på grunnlag av en risikovurdering
  - ”Betydelig” eller ”Høyt” - Nkom
- Ikke fellesbruker for tilgang til helse- og personopplysninger
- Alle standardpassord (fabrikkinnstillinger) på systemer og utstyr skal endres
- Ved bruk av trådløse nettverk skal den autoriserte brukeren autentiseres med sikker autentiseringsløsning

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

Kontroll av tilgang og tildelte autorisasjoner

- **Jevnlig** kontroll av hvem som har hatt tilgang
- Gjennomgang og kontroll av tilgangsstyring, herunder **tildelte autorisasjoner**, skal foretas av den enkelte leder:
  - 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

Kontroll av:

- **Hvem som har hatt tilgang**
- **Tildelte autorisasjoner**
  - **F.eks brukere som har sluttet**

Logging (1)

- 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
- Fra kap 4.2.3 Innsyn:
  - Virksomheten skal sikre at den registrerte kan få innsyn i opplysninger registrert om seg selv. Dette innsynet **gjelder også loggen** over hvem, og fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt.

Logging (2)

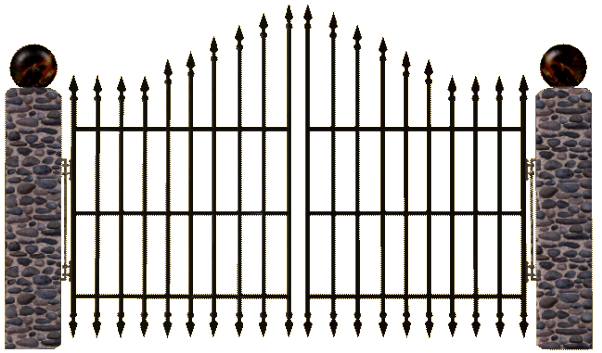
- Følgende skal som minimum registreres i loggene ved autorisert bruk av behandlingsrettet helseregister:
  - Identiteten til den som har lest, rettet, registrert, endret og/eller slettet opplysninger
  - Organisatorisk tilhørighet
  - Grunnlaget for tilgjengeliggjøringen
  - Tidsperioden for tilgjengeliggjøringen
- 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 (3)

- 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

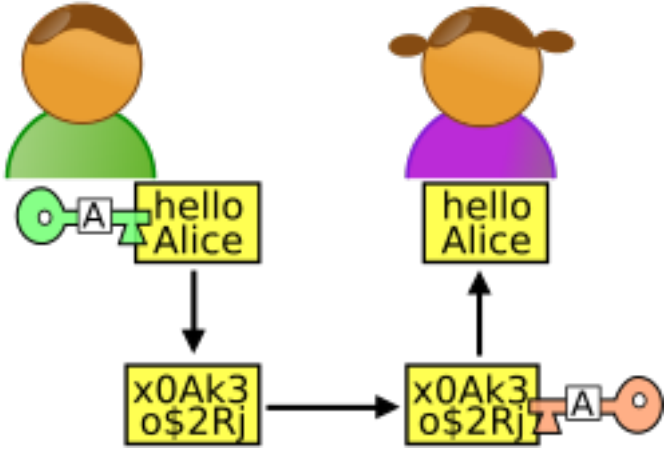
Kap 5.3 Fysisk sikkerhet og håndtering av utstyr (1)

- Sikkerhetstiltak skal hindre at uautoriserte får tilgang til helse- og personopplysninger.
- Det skal etableres rutine for administrasjon av nøkler/adgangskort i adgangskontrollsystemet.
- Adgangskontroll av lokaler med utstyr (Husk medisinsk utstyr!)
- utstyret sikres mot misbruk eller uautorisert innsyn.
- hindre at annet enn autorisert personell får adgang til infrastruktur.
- Alle lagringsmedier skal slettes forsvarlig når de tas ut av bruk.
- Risikovurdering og rutiner før mobilt utstyr og hjemmekontor tas i bruk
- Helse- og personopplysninger skal bare lagres lokalt på utstyret når dette er nødvendig ut fra tjenstlig behov, og skal alltid lagres kryptert.



Kryptering

- Tekniske tiltak skal etableres slik at all kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll krypteres
- Kryptering og dekryptering mellom kommunikasjonspunkter i infrastrukturen skal gjøres i godkjent utstyr virksomheten har kontroll med.
  - **Kontrollen kan ivaretas gjennom avtale.**
- All kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer, skal sikres ved kryptering
- Kryptering av lagrede helse- og personopplysninger kan vurderes som et sikkerhetstiltak.



5.4 Sikker IT-drift

- Konfigurasjonskontroll
  - Det er en forutsetning at virksomheten har **oversikt** over dataflyt, datakommunikasjon og integrasjoner og kontroll på alt eget utstyr og programvare som benyttes i behandlingen av helse- og personopplysninger.
  - Se også Kap 3.3 oversikt over IKT-systemer, infrastruktur m.m

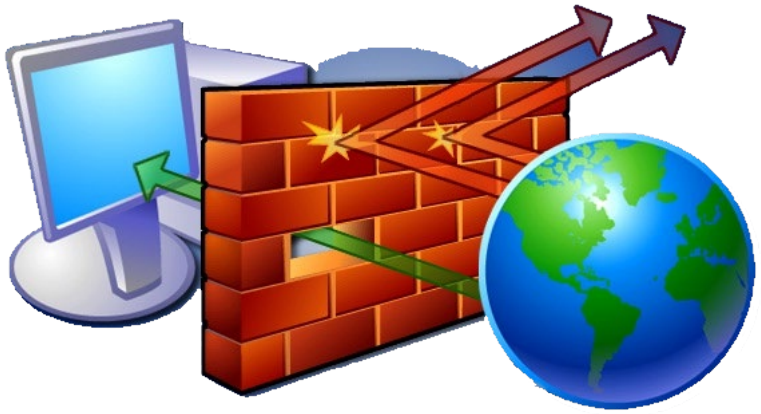
- Endringsstyring
  - Alle **endringer** med betydning for informasjonssikkerheten i organisasjon, informasjonssystem og infrastruktur skal **forankres** på relevant ledernivå.

- Sikkerhetskopiering

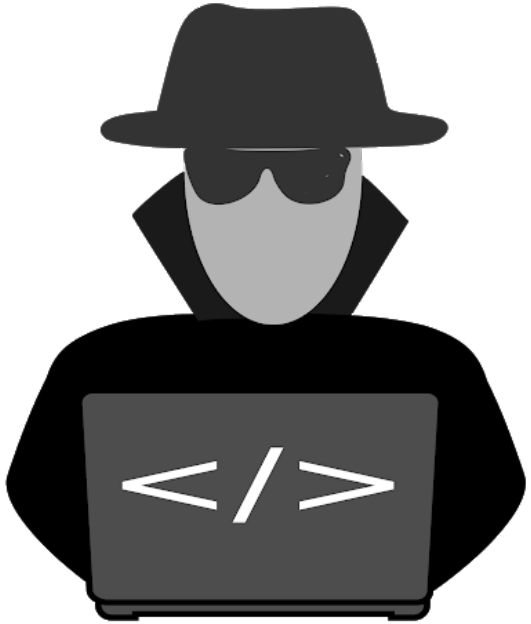
- Styring og håndtering av tekniske sårbarheter
  - Virksomheten skal ha rutine for å **skaffe seg informasjon om tekniske sårbarheter** i utstyr og programvare.
  - Også rutiner for bl.a. hvordan virksomheten skal **reagere og varsle** om sårbarheter

5.5 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



5.4.6 Sikkerhetsrevisjon
5.8 Håndtering av informasjonssikkerhetsbrudd



- Virksomhetens ledelse skal følge opp at sikkerheten ivaretas ved jevnlige og **minimum årlige sikkerhetsrevisjoner**.
- Uønskede hendelser (for eksempel brudd på rutiner, personvernet eller informasjonssikkerheten) skal behandles som **avvik**. Avvik skal behandles for å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse.
- Dersom avviket er et **brudd på personopplysningssikkerheten** og har eller vil føre til middels eller høy risiko for den registrerte, skal avviket rapporteres til **Datatilsynet** innen 72 timer.
- Dersom det er sannsynlig at avviket har eller vil føre til høy risiko for **den registrerte**, skal virksomheten underrette vedkommende.

- Alvorlig svikt i informasjonssystemer kan være meldepliktige til Statens Helsetilsyn

5.9 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