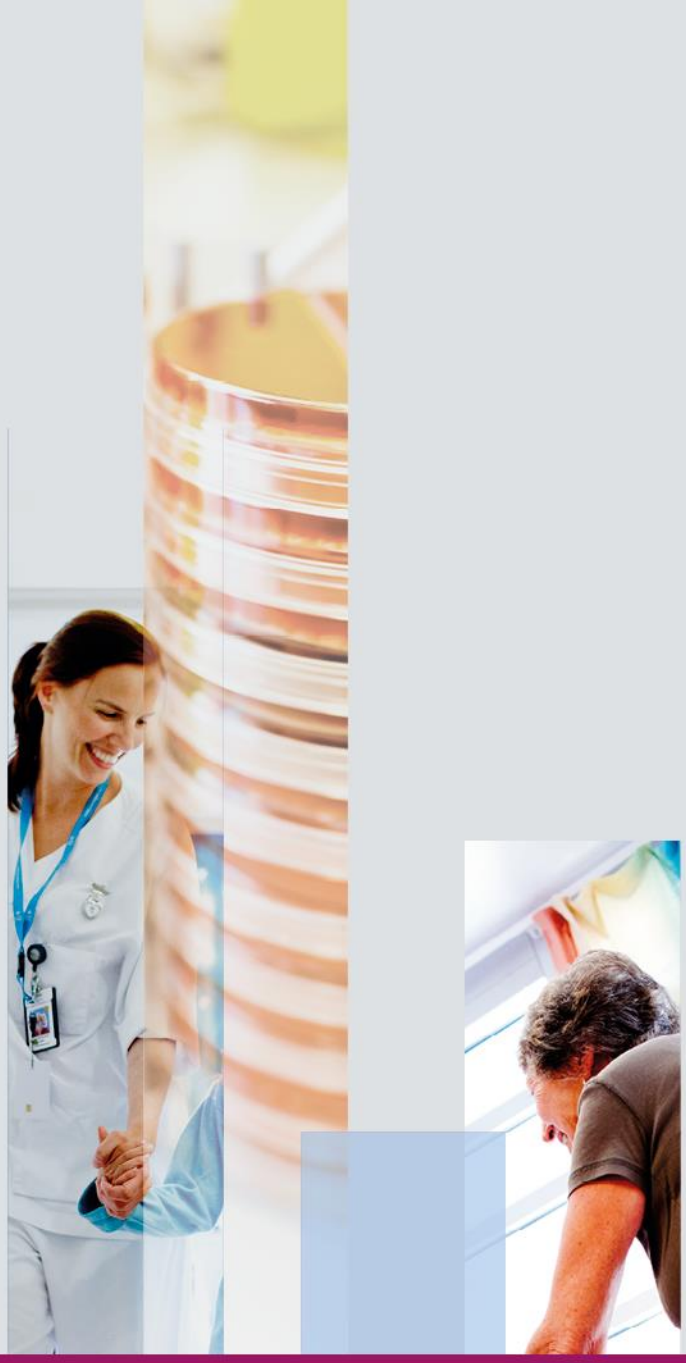
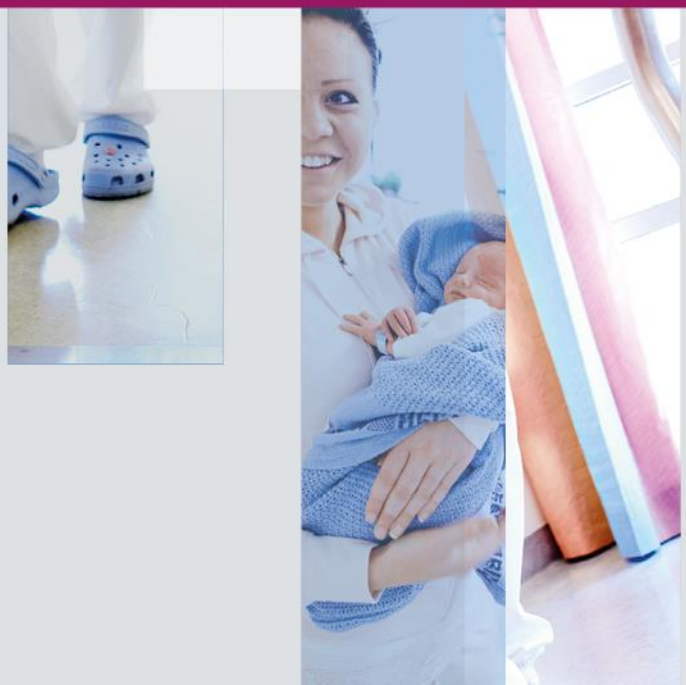


Personvern- og informasjonssikkerhetsstrategi 2023 - 2026



SYKEHUSET I VESTFOLD

Innholdsfortegnelse

Om strategien[1]

Sykehuset i Vestfold (sykehuset) er dataansvarlig for behandling av store mengder personopplysninger hvorav en vesentlig del er av sensitiv art [1]. Det behandles også mengder av virksomhetsdata av sensitiv og kritisk art [2].

Som dataansvarlig plikter sykehuset å etterleve personvernregelverket. Sykehuset har også forpliktet seg til å følge Normen [3]. Det er en bransjenorm som er utarbeidet og forvaltes av organisasjoner og virksomheter i helse- og omsorgssektoren. Normen skal, innenfor lovverkets rammer, søke en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet.

Sykehuset har også forpliktet seg til å følge det regionale ledelsessystemet for informasjonssikkerhet basert på ISO 27001 [4] [5]. Denne internasjonale standarden er utarbeidet for å stille krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet.

For å sikre etterlevelse og oppnå best mulig personvern og informasjonssikkerhet, er det behov for strategisk jobbing og prioritering av oppgavene. Sykehusets «Personvern- og informasjonssikkerhetsstrategi 2023 – 2026» skal bidra til dette.

Strategien bygger på «Nasjonal strategi for digital sikkerhet» som regjeringen lanserte i 2019. [6]

Fra innledningen:

> *Digitaliseringen av det norske samfunnet utfordrer oss også. Digitale infrastrukturer og systemer blir stadig mer komplekse, omfattende og integrerte. Det skapes avhengigheter og sårbarheter på tvers av ansvarsområder, sektorer og nasjoner. Det forventes at digitale tjenester skal være tilgjengelige til enhver tid. En vellykket digitalisering handler også om at løsningene ivaretar krav til sikkerhet og den enkeltes personvern på en god måte, og at vi kan ha tillit til at digitale løsninger fungerer slik de skal.*

I arbeidet med strategien er det sett hen til øvrige strategier i sykehuset som eksplisitt inneholder «personvern» og eller «informasjonssikkerhet/IKT-sikkerhet»:

- *Teknologistrategien* har i «**Tiltaksområde 2 – Integrerte helsetjenester**» [7]
  - Mål: SiV preges av brukervennlige løsninger som fremmer fornuftig tidsbruk og fokus på informasjonssikkerhet
    - Hovedtiltaket vil være: Forsterke arbeidet med tilgjengelighet og integritet innen informasjonssikkerhet og personvern.

[1] Kildereferanser er viktige for integritet, sporbarhet og annerkjennelse av andres arbeid. I denne strategien brukes tall i klammeparentes i teksten, for eksempel [99]. Referansene finner man igjen i referanselisten på siste side av denne strategien.

- *Kompetansestrategien* har i sitt «**Hovedmål 4: Sykehusets teknologikompetanse er styrket og potensialet i ny teknologi utnyttes**» [8].
  - «Det vil være viktig å ha god bestillerkompetanse slik at sykehuset kan påvirke løsningene til å bli gode støtteverktøy for klinikere og andre ansatte. Sykehuset må ha kompetanse på fagområder som virksomhet- og systemarkitektur, personvern, IKT-sikkerhet, brukervennlighet og god design.»

- *Forsknings- og innovasjonsstrategien* fastsetter våre **kontinuerlige mål og oppgaver innen forskning og innovasjon** [9]:
  - God forskningskultur skal prege virksomheten, gjennom ledelsesmessig og kollegial tilrettelegging for forskning. Nasjonal lovgivning, internasjonalt aksepterte retningslinjer, god forskningsetikk og personvern skal ligge til grunn for all forskning ved sykehuset. En viktig del av forskningskulturen skal være økt involvering av brukere (eg. pasienter, pårørende) i klinisk forskning.

Selv om «*Plan for pasientsikkerhet og kvalitet 2019 – 2023*» eksplisitt ikke inneholder «personvern» og eller «informasjonssikkerhet/IKT-sikkerhet», så er utgangspunktet at informasjonssikkerhet er pasientsikkerhet [10]. Pasientsikkerhet er mer enn korrekt behandling av pasienten. Det er også å sørge for at personopplysninger behandles slik at deres integritet, tilgjengelighet og konfidensialitet beskyttes samt sørge for at alle informasjonssystemer tåler angrep (robusthet). Grunnleggende handler informasjonssikkerhet og personvern om å ivareta befolkningens tillit til helsevesenet.

I arbeidet med strategien er det også tatt utgangspunkt i kartleggingen som Statens helsetilsyn gjennomførte i 2020 av kritiske system, risikovurderinger og nødrutiner for IKT-system ved 17 norske sykehus, inkl. SiV [11]. Funn i kartleggingen viser at virksomhetene har utarbeidet mange risikoanalyser for IKT-endringer. Men det er utarbeidet få overordnede risikovurderinger for bortfall av all IKT. De fleste risikoanalyser har fokus på tekniske forhold, men lite på konsekvenser av IKT-bortfall i klinisk virksomhet.

Det er utarbeidet fem, overordnede strategiske mål som skal være styrende for sykehusets arbeid innen personvern og informasjonssikkerhet i perioden 2023 – 2026.

De strategiske målene skal bidra til å øke kompetanse, bygge kultur og gi en bedre risikoforståelse innen disse fagområdene. Strategien følges opp gjennom rullerende handlingsplaner og årshjul.

Fra nasjonal strategi for digital sikkerhet:

Nå starter den viktigste jobben – oppfølgingen. Jeg håper dere tar eierskap til den nye nasjonale strategien for digital sikkerhet, setter strategien på dagsorden og bidrar til at den følges opp. Ved å møte digitale sikkerhetsutfordringer på en god måte, kan vi få større utbytte av de positive mulighetene digitaliseringen gir oss som enkeltmennesker, virksomheter og som samfunn.

Tidligere statsminister Erna Solberg (2019)

Visjon og verdier

Sykehusets og foretaksgruppens visjon er å skape gode og likeverdige helsetjenester til alle som trenger det, når de trenger det, uavhengig av alder, bosted, etnisk bakgrunn, kjønn og økonomi [12].

Sykehusets verdier er:

- Kvalitet
- Trygghet
- Respekt

Informasjonsbehandlingen skal understøtte helseforetakenes oppgaver og tjenester innen pasientbehandling, forskning, undervisning og pasient- og pårørendeopplæring, slik at helseforetakenes mål nås. Informasjonsbehandlingen skal legge til rette for gode og sammenhengende pasientforløp, også på tvers av helseforetak og omsorgsnivåer.

Informasjonsbehandlingen omfatter også kommunikasjon med pasienter, brukere og pårørende, blant annet for at pasienter skal kunne medvirke i egen behandling.

Helse Sør-Øst (HSØ) sitt overordnede styrende dokument «Mål og strategi for informasjonssikkerhet» tar for seg «*Omfang*», «*Formålet med informasjonsbehandlingen*», «*Mål for informasjonssikkerhet*» og «*Strategi for informasjonssikkerhet*», som skal bidra til å understøtte regionens visjoner [13].

«Mål og strategi for informasjonssikkerhet» inneholder krav som tas med videre i strategien som strategiske mål og er blant annet:

- Ledelsessystem for informasjonssikkerhet skal være en del av internkontrollen for helhetlig risikostyring i helseforetakene [4]
- Informasjonssikkerhetsarbeidet skal være risikobasert
- Ansvar og myndighet for informasjonssikkerhet følger det ordinære linjeansvaret

Strategiske mål

Som oppfølging og videreføring av regionens strategiske dokumenter innenfor personvern og informasjonssikkerhet er det behov for mer langsiktig og strategisk arbeid innenfor områdene personvern og informasjonssikkerhet i sykehuset. Det er plukket ut fem strategiske innsatsområder som det fokuseres på i strategiperioden.

- Styring og forbedring
- Risikohåndtering
- Organisering
- Systemeierskap
- Kultur og bevisstgjøring

Mål 1 - Styring og forbedring

Sykehuset skal ha et ledelsessystem for informasjonssikkerhet (internkontroll). Kravet fremgår av personvernregelverket, Normen og det regionale ledelsessystemet for informasjonssikkerhet.

Sykehusets visjon for styring og forbedring av personvern- og informasjonssikkerhetsarbeidet:

Sykehuset skal videreutvikle ledelsessystem for personvern- og informasjonssikkerhet til beste for pasienter, ansatte og andre brukere.

Personvern og informasjonssikkerhet i sykehuset skal styres og forbedres slik:

- Implementere regionale føringer for informasjonssikkerhet for personvern og informasjonssikkerhet i sykehusets ledelsessystem
- Harmonisere mot ISO 27001 og 27002:2022, supplere med anerkjente grunnprinsipper for IKT-sikkerhet der ISO ikke fyller godt nok ut
- Kontinuerlig forbedre internkontrollaktiviteter på området
- Årlige kontroller og revisjoner
- Bidra inn i forvaltningen av artikkel 30 «Protokoller over behandlingsaktiviteter» [14]
- Bidra til å utvikle en «IKT-journal» for å ivareta informasjon ifm. livssyklusen til et informasjonssystem

Mål 2 - Risikohåndtering

Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte.

En risikovurdering er et verktøy for å identifisere uønskede hendelser og risikoen for at disse skal inntreffe. Som en del av internkontrollen skal sykehuset ha en oversikt over hvilke behandlinger av personopplysninger som foretas, og hvilke personopplysninger som inngår i disse. Denne oversikten skal brukes som underlag ved risikovurderinger.

Personvern- og informasjonssikkerhetsrisikoer er faktorer som kan påvirke all virksomhet i sykehuset. Å eliminere all risiko er umulig, men det er viktig å håndtere restrisiko på en god måte. Beslutningstagere må ha tilstrekkelig kunnskap om risiko til å ta informerte beslutninger. Derfor er det viktig å utvikle metoder og prosesser for å finne, analysere og vurdere risiko. Når risikoer er identifisert, analysert og vurdert har sykehuset tilstrekkelig kunnskap til å håndtere restrisiko.

Sykehusets visjon for håndtering av personvern- og informasjonssikkerhetsrisiko:

Sykehuset sine beslutningstagere skal ha kunnskap om personvern- og informasjonssikkerhetsrisikoer innen sine ansvarsområder.

Sykehuset skal håndtere risiko ved å:

- Gjennomføre årlige risikovurderinger for sykehuset
- Sykehuset skal ha god oversikt over de høyeste risikoene
- Vurdere risiko ved innføring av nye informasjonssystemer og prosesser, og gjennomføre personvernkonsekvensvurderinger (DPIA) der hvor det foreligger høy risiko for den registrertes personvern
- Etablere et informasjonssystem for systematisk oppfølging av risikorestanser for alle informasjonssystemer og prosesser
- Risikoreduserende tiltak skal velges basert på risikovurderinger, vesentlighet, kost-nytte-vurderinger og ledelsens føringer for risikohåndtering, samt effektiv sikkerhetsarbeid
- Forankre restrisiko i linjen
- Ressursinnsatsen skal tilpasses risiko, der høy risiko vurderes grundigere enn lav risiko
- Styrke lærings- og forbedringspotensialet som ligger i uønskede personvern- og informasjonssikkerhetshendelser

Mål 3 - Organisering

Sykehuset er ansvarlig for behandling av personopplysninger som skjer i sykehuset og for å ivareta informasjonssikkerheten. Ansvar og myndighet for informasjonssikkerhet følger det ordinære linjeansvaret. Det omfatter utøvende og kontrollerende ansvar / oppgaver, herunder utpeking av hvilken risiko hver rolle er ansvarlig for.

Det er et fåtall ansatte som har personvern og informasjonssikkerhet som sine hovedoppgaver i sykehuset. Det er personvernombud og informasjonssikkerhetsleder, men ingen rådgivere på fagområdene. Det finnes noe kompetanse på informasjonssikkerhet i IKT og ehelseavdelingen.

De fleste ansatte i sykehuset behandler personopplysninger daglig. I tillegg er det flere prosjektdeltagere som er med på å utvikle informasjonssystemer der personopplysninger skal behandles i henhold til personvernprinsippene [15]. Risiko for uønskede hendelser (tilsiktet eller utilsiktet) kan påvirke hvordan vi klarer å løse vårt samfunnsoppdrag over tid.

Ressursene innen personvern- og informasjonssikkerhet har som oppgave er å gi råd slik at alle i sykehuset kan utføre sine oppgaver på en god måte. Dette krever både at det er tilstrekkelig kompetanse i organisasjonen vår til å etterspørre råd til rett tid, og tilstrekkelig ressurser til å svare.

Sykehusets visjon for organisering av personvern- og informasjonssikkerhetsarbeidet er:

Sykehusets personvern- og informasjonssikkerhetsarbeid skal bidra til bedre tjenester for pasienter, ansatte og andre brukere.

Sykehuset skal utvikle organisasjonen ved å:

- Styrke samarbeidet mellom ressursene innen personvern- og informasjonssikkerhet og klinikkene/divisjonene, staber og prosjektdeltagere
- Styrke personvern- og informasjonssikkerhetskompetansen i sykehuset
- Bidra i utviklingen av roller og samarbeid om personvern og informasjonssikkerhet
- Utvikle gode forløp for saksbehandlingen av personvern- og informasjonssikkerhetssaker

Mål 4 - Systemeierskap

Med stadig nye teknologier som skyløsninger, hjemmebasert sykehusbehandling (Digital hjemmeoppfølging (DHO)) og sensorbasert oppfølging av pasienter, endrer dette måten sykehuset samler inn og behandler personopplysninger. Ofte utvikles og implementeres systemer i samarbeid med eksterne leverandører. Denne utviklingen utfordrer sykehusets tradisjonelle rolle som pasientbehandler, arbeidsgiver og systemeier.

For systemeier holder det ikke at et system fungerer teknisk. Bruken av systemene må bidra til bedre helsetjenester eller interne prosesser. Systemeiere vil ha ansvaret for risiko knyttet til systemet de er ansvarlige for, og vil derfor også være risikoeiere.

Sykehusets visjon for systemeierskap:

Sykehuset sine systemeiere skal sørge for tilstrekkelig personvern og informasjonssikkerhet i informasjonssystemer og løsninger.

Sykehuset skal etablere systemeierskap ved å:

- Utvikle systemeierskapsrollen i sykehuset
- Styrke systemeiers kompetanse til å beskytte informasjon som behandles i informasjonssystemene mot ulovlig innsyn og endring
- Oppfylle personvernprinsippene i informasjonssystemer og løsninger
- Ivareta de registrertes rettigheter
- Utvikle metoder for å identifisere restrisiko i nye og gamle informasjonssystemer
- Oppdatere kost-nytte-vurderinger gjennom informasjonssystemers livsløp

Mål 5 - Kultur og bevisstgjøring

Alle ansatte, uansett arbeidsforhold i sykehuset må ha tilstrekkelig kunnskap om og evne til å gjøre valg om personvern og informasjonssikkerhet som sikrer konfidensialitet, integriteten og tilgjengelig til all informasjonen (data) vi samler inn og behandler.

For å ta de rette valgene må kulturen i sykehuset preges av at personvern og informasjonssikkerhet vektes opp mot pasientbehov, pasientsikkerhet og andre behov når vi behandler informasjonen.

Personopplysninger kommer i mange former. De kan trykkes eller skrives på papir, lagres elektronisk, overføres via post eller elektroniske media, eller formidles muntlig. Uansett hvordan informasjonen behandles, skal den alltid beskyttes på en tilfredsstillende måte. Sykehusets kultur og bevisstgjøring skal ikke bare inneholde en digital sikkerhetskultur, men også ta med seg den analoge delen som skjer når det f.eks. behandles noe på papir.

Sykehusets visjon for personvern- og informasjonssikkerhetskultur:

Sykehuset skal skape en sikkerhetskultur til det beste for pasienter, ansatte og samfunnet.

Personvern- og informasjonssikkerhetskulturen skal bygges ved:

- Årlige bevisstgjøringskampanjer for alle ansatte, som ved f.eks. sikkerhetsmåneden [16]
- Videreføre bevisstgjøringskampanjer gjennom hele året
- Opplæring av nyansatte
- Opplæring av ledere
- Veilede og kurse
- Alle klinikker / avdelinger skal sette egne mål innen personvern- og informasjonssikkerhet

Viktige ord og uttrykk i personvern- og informasjonssikkerhetsarbeidet

Personvern
Personvern omhandler det enkelte menneskets ukrenkelighet og krav på respekt fra andre mennesker, respekt for egen integritet og privatlivets fred. Personvern er derfor nært knyttet til enkeltindividers muligheter for privatliv, selvbestemmelse og selvutfoldelse.

Retten til privatliv følger blant annet av den europeiske menneskerettskonvensjon (EMK) artikkel 8 og står sentralt i EUs personvernforordning (2016/679). Disse internasjonale regelsettene ligger til grunn for Grunnloven § 102 hvor personvernet kommer til uttrykk som en rett til privatliv og i vår nasjonale personvernlovgivning.

Informasjonssikkerhet
Med informasjonssikkerhet m enes evnen til å beskytte informasjonssystemer og opplysninger mot at de eksponeres for uvedkommende (*konfidensialitet*), skades eller ødelegges, endres eller slettes på uautoriserte måter (*integritet*) eller er utilgjengelige for rettmessige brukere (*tilgjengelighet*) og organisasjonens evne til å gjenopprette normaltilstanden (*robusthet*).

Informasjonsverdier
Mange benytter begrepet «informasjonsverdi» som et samlebegrep som inkluderer både informasjon og tilhørende støtteverdier som IKT-system, digitale tjenester, datautstyr av ulike varianter mv. Støtteverdiene er «noe» som benyttes i behandlingen av informasjonen.

Personopplysninger
Personopplysninger er alle opplysninger og vurderinger som kan knyttes til en identifisert eller identifiserbar fysisk person.

Særlige kategorier av personopplysninger
Personopplysninger av særlig kategori (sensitive) er vurderinger og opplysninger som kan knyttes til bestemte enkeltpersoner og som krever et særskilt vern.

Helseopplysninger og helserelaterte forhold, genetiske og biometriske opplysninger med det formål å entydig identifisere en fysisk person, etnisk eller rasemessig opprinnelse, politiske, filosofiske eller, religiøse oppfatninger og livssyn, seksuell orientering eller seksuelle forhold, fagforeningsmedlemskap

Dataansvarlig / behandlingsansvarlig
Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Dette er vanligvis en virksomhet.

Databehandler
Den som behandler personopplysninger på oppdrag fra den behandlingsansvarlige. Dette er vanligvis en virksomhet.

DPIA
En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal sikre at personvernet til de som er registrert i informasjonssystemet/løsningen ivaretas. Dette er en plikt etter personvernregelverket.

Artikkel 30-protokoll
Alle virksomheter som behandler personopplysninger, skal føre en protokoll over behandlingsaktivitetene de har ansvar for.

Behandling av personopplysninger
Med behandling av personopplysninger menes alle typer bruk av personopplysninger, som for eksempel: innsamling, registrering, lagring, sammenstilling, bruk, overføring, publisering, sletting. Sykehuset plikter å holde oversikt over all behandling av personopplysninger. Hver behandling skal derfor registreres i sykehusets protokoll over behandlingsaktiviteter

ISO 27001 og 27002
Denne internasjonale standarden er utarbeidet for å stille krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet.

Normen
Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) er et omforent sett av krav til informasjonssikkerhet basert på lovverket. Normen er en bransjenorm for informasjonssikkerhet og personvern og utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren.

Referanser

[1] Definisjon: https://lovdata.no/lov/2018-06-15-38/gdpr/a9

[2] Virksomhetsdata som ikke inneholder personopplysninger, eks. service og driftsanlegg (SD-anlegg), kontrakter, anbud, økonomi, skallsikring, plassering av følsomt utstyr m.m.

[3] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen)

[4] Ledelsessystem for informasjonssikkerhet - Helse Sør-Øst RHF (helse-sorost.no)

[5] NS-EN ISO/IEC 27001 Informasjonssikkerhet - Krav | standard.no

[6] Nasjonal strategi for digital sikkerhet - regjeringen.no

[7] Teknologistrategi (sykehuspartner.no)

[8] Kompetansestrategi 2019 - 2023 - dok25771.pdf

[9] Forsknings- og innovasjonsstrategi 2019 - 2022 - dok15724.pdf

[10] Plan for pasientsikkerhet og kvalitet 2019 - 2023 - dok25178.pdf

[11] Forsvarlig pasientbehandling uten IKT? | Helsetilsynet

[12] Om Sykehuset i Vestfold - Sykehuset i Vestfold (siv.no)

[13] Mål og strategi for informasjonssikkerhet i Helse Sør-Øst – overordnet styrende dokument (helse-sorost.no)

[14] https://lovdata.no/lov/2018-06-15-38/gdpr/a30

[15] Personvernprinsippene | Datatilsynet

[16] Nasjonal sikkerhetsmåned | Digdir