HELSE MIDT-NORGE

Sikkerhetsprinsipper og -krav for IKT-infrastruktur og -tjenester

Versjon	**Dato**	**Endring**	**Godkjent av**
1.0	02.06.2021	Første versjon	Regional eiergruppe for informasjonssikkerhet og personvern
1.1	10.03.2022	Korrigering av avsnittsnummer i kap. 3.3 og 3.15	

1. Hensikt og omfang

Sikkerhetsprinsipper og –krav for IKT-infrastruktur og -tjenester, inkludert behandlingsrettede helseregistre, er en sammenstilling av nødvendige prinsipper og krav for å oppnå tilfredsstillende informasjonssikkerhet i Helse Midt-Norges (HMN) infrastruktur og IKT-tjenester.

Dokumentet detaljerer valgene og føringene HMN har satt i sikkerhetsmålene og sikkerhetsstrategien.

1.1. Målgruppe

Målgruppen for dokumentet er beslutningstakere, informasjonssikkerhetsledere, personvernombud, regionalt informasjonssikkerhetsforum (RIF), Tjenesteutviklere, systemeiere og prosjektene, i HMN.

1.2. Hvordan bruke dokumentet

Dokumentet kan brukes som sjekkliste sammen med et løsningsdesign i forbindelse med etablering av tjeneste, endring av tjenester, eller i forbindelse med revisjoner og internkontroll og risiko- og sårbarhetsvurderinger (ROS).

Dokumentet skal brukes som grunnlag ved anskaffelser. Deler av kravene i dette dokumentet er spesifikt rettet mot behandlingsrettede helseregistre. Disse vil ikke være relevante for andre system. Dokumentet kan utleveres til leverandører for å synliggjøre krav i en anskaffelsesprosess.

1.3. Unntak fra sikkerhetsprinsipper og –krav

Unntak fra kravene i dette dokumentet skal dokumenteres og godkjennes av dataansvarlig. Grunnlaget for å beslutte unntak skal dokumenteres i form av risikovurdering. I de tilfellene et eventuelt unntak vil kunne påvirke flere tjenester eller øvrig sikkerhet i HMN, skal unntaket drøftes i RIF og godkjennes av samtlige virksomheter i HMN.

1.4. Forrang over andre dokumenter

Dette dokumentet er underordnet NO-5 sikkerhetsmål og nivå for akseptabel risiko for informasjonssikkerhet samt NO-6 sikkerhetsstartegi, og disse dokumentene har ved en ev. konflikt forrang.

I tilfelle konflikt med andre styrende dokumenter, må det avklares med informasjonssikkerhetsleder ved berørt foretak hvilket dokument som har forrang.

2. Ansvar

- **Virksomheten v/ administrerende direktør** er dataansvarlig for all behandling av helse- og personopplysninger med tilknytning til virksomheten Administrerende direktør er videre endelig ansvarlig for informasjonssikkerhet i egen virksomhet.
- **Ledere** på alle nivåer har ansvar for etterlevelse av dokumentet i egen enhet.
- **Ansatte og innleide** med beslutningsmyndighet og/eller ansvar for systemer og/eller anskaffelser er ansvarlig for å etterleve dette dokumentet.

3. Sikkerhetsprinsipper og –krav

3.1. Behandling av helse- og personopplysninger

Med behandling av helse- og personopplysninger menes all registrering, prosessering, bruk og lagring av helse- og personopplysninger som gjøres. Det er dataansvarlig som beslutter formålet med databehandlingen. Hemit i sin rolle som databehandler for virksomheten utfører databehandling etter avtale med virksomheten (dataansvarlig).

Helse- og personopplysninger skal slettes når formålet med behandlingen er oppfylt og det ikke i loven er oppstilt krav om videre lagring. Sletting involverer en fullstendig sletting av opplysninger, fra alle medier opplysningene er lagret på. Arkivlovens regler vil ofte tilsi at helseopplysninger ikke skal slettes, men arkiveres.

- Behandling av helse- og personopplysninger skal gjøres i tråd med reglene i personopplysningsloven og tilhørende personvernforordning.
- Begrepet helse- og personopplysninger omfatter både direkte og indirekte identifiserbare opplysninger.

Krav for databehandling	
3.1.1	Dataansvarlig skal beslutte og godkjenne et formål med og et behandlingsgrunnlag for databehandlingen.
3.1.2	Dataansvarlig er ansvarlig for at det er gjennomført personvernkonsekvensvurdering (DPIA) der det er påkrevd etter lov.
3.1.3	Det skal være opprettet og godkjent en tjenesteavtale/oppdragsavtale og databehandleravtale mellom Databehandler og Dataansvarlig for databehandling knyttet til tjenesteavtalen/oppdragsavtalen. For databehandling som går ut over tjenesteavtalen må det foreligge instruks fra dataansvarlig.
3.1.4	Det skal være opprettet og godkjent databehandleravtaler med eventuelle underleverandører som behandler personopplysninger.
3.1.5	Det skal det være definert en systemeier og en tjenesteutvikler for behandlingen.

3.2. Særlig for Anskaffelser

Ved anskaffelser skal virksomheten(e) sørge for at leverandører og utstyr i best mulig grad etterlever sikkerhetskravene beskrevet i dette dokumentet. Beskyttelse av data og helse- og personopplysninger skal sikres slik det kreves i relevante lover, forskrifter, og kontraktsbestemmelser.

Sikkerhetskrav ved anskaffelser	
3.2.1	Utforming, drift, bruk og administrasjon av informasjonssystemer skal samstemme med aktuelle lover, forskrifter og kontraktsfestede krav til sikring.
3.2.2	Anskaffelsen skal være i tråd med HMNs styringssystem for informasjonssikkerhet og personvern.

3.2.3	Systemer som anskaffes med underliggende komponenter skal supporteres i kontraktsperiodens levetid.

3.3. Brukerkontoer

Med brukerkonto menes en representasjon av en digital identitet. Alle ansatte i virksomheten skal ha en personlig konto. Tilgang til informasjon, informasjonsbehandlingsutstyr og virksomhetsprosesser skal kontrolleres på grunnlag av virksomhetsbehov, tjenstlig behov og sikkerhetsbehov.

Sikkerhetskrav for brukerkontoer	
3.3.1	Det skal kun benyttes personlige brukere[1]. Fellesbrukere eller på annen måte deling av brukerkontoer skal ikke forekomme.
3.3.2	Brukerkontoer skal entydig knyttes opp mot den digitale identitet til den enkelte og ivareta uavviselighet og sporbarhet ved autentisering.
3.3.3	En brukers tilgang til tjenester og informasjon skal slettes når tjenstlig behov for dette opphører.
3.3.4	Brukerkontoer skal slettes etter arbeidsforholdet er opphørt.
3.3.5	Brukerkontoer skal ikke gis administrative rettigheter. For dette formålet skal personlige administratorkontoer opprettes.
3.3.6	Brukerkontoer skal følge regional passordpolitikk.
3.3.7	Kravene til passordlengde og -kompleksitet skal håndheves automatisk av systemet. Dette gjelder alle kategorier brukeridentiteter, inkludert system og servicekontoer.
3.3.8	Brukere skal hindres i å benytte informasjonsbehandlingsutstyr til ikke-autoriserte formål.
3.3.9	Varigheten av aktive sesjoner skal tidsavgrenses for å forhindre brukerne fra å holde sesjonene åpne slik at ny autentisering kan unngås.
3.3.10	Det skal gjennomføres opplæring i policy og prosedyrer som er relevant for brukere av systemet. Dette gjelder alle brukere og administratorer av systemet, samt eventuelle kontraktører og tredjepartsbrukere.

Spesielt for behandlingsrettede helseregistre	
3.3.11	Arbeidsforholdet[2] til den enkelte skal være entydig identifiserbart så lenge bruker er pålogget og kunne spores i de behandlingsrettede helseregistre den enkelte er gitt tilgang til.

[1] Dette påvirker ikke muligheten til å beslutte opprettelse av system- og servicekontorer som benyttes av IKT-systemer eller tjenester til å utføre automatisk funksjonalitet (typisk back-up, antivirus, oppgraderinger etc.) som ikke har tilgang til helse- og personopplysninger.

[2] Dette kan løses på ulike måter f.eks. vha. en kombinert primærnøkkel som alltid består av en ansatt- og en organisasjonsidentifikator. Arbeidsforholdet omfatter både fast- og deltidsansatte, samt innleide og andre som foretaket har ordnet formell instruksjonsrett over for og registrert i HR-systemet.

3.3.12	Det skal være mulig å entydig identifisere hvem som er arbeidsgiver til den enkelte ansatte (entydig identitet). Dersom det foreligger flere ansettelsesforhold skal applikasjonen sørge for at det er entydig i hvilket forhold den ansatte til enhver tid opptrer.
3.3.13	Identiteten til den enkelte som bruker ett eller flere behandlingsrettede helseregistre skal være gjennomgående sporbar på tvers av disse.
3.3.14	Autentisering skal støtte identitetsutveksling ved hjelp av OAuth 2.0 eller tilsvarende teknologi forsterket med kryptografisk signering.
3.3.15	Den autoritative kilden for ansattidentiteter skal være det regionale lønns- og personalsystemet.
3.3.16	Den autoritative kilden for organisasjonsenheter i spesialisthelsetjenesten skal være det til enhver tid gjeldende nasjonale helseadministrative register (p.t. Register over Enheter i Spesialisthelsetjenesten[3]).
3.3.17	Programvare som krever systemkonti av ulike slag skal ikke ha systemkonti som kan brukes til å få tilgang til innholdet i det behandlingsrettede registeret eller tilgang til å opprette nye brukere i systemet.

3.4. Personlige administratorkontoer

Sikkerhetsprinsipper for personlige administratorkontoer	
3.4.1	Personlige administratorkontoer skal kun benyttes for å oppnå eller utføre administrative oppgaver.
3.4.2	Administratorkontoer skal knyttes opp mot en digital identitet, slik at kravet om uavviselighet og sporbarhet ivaretas.
3.4.3	Administratorkontoer skal følge regional passordpolitikk.
3.4.4	Kravene til passordlengde og -kompleksitet skal håndheves automatisk av systemet.
3.4.5	Administratortilgang skal begrenses iht. dokumentert behov.
3.4.6	Administratorkontoer skal deaktiveres når behovet bortfaller.

3.5. Upersonlige system- og administratorkontoer

Med upersonlige system- og administratorkontoer menes kontoer som ikke er knyttet til person, dvs. kontoer som «root», «db_admin», «administrator» og så videre, samt også servicekontoer. Tilgang til disse skal begrenses.

Sikkerhetsprinsipper for upersonlige system- og administratorkontoer	
3.5.1	System- og administratorbrukere skal opprettes i tråd med HMNs passordpolitikk
3.5.2	System- og administratorpassord skal inngå i virksomhetens passordhvelv.
3.5.3	Det skal foreligge en oversikt over hvem som har tilgang til og tillatelse til å benytte upersonlige system – og administratorkontoer.

[3] For tiden er RESH den autoritative datakilden for organisasjonsenheter i spesialisthelsetjenesten

3.6. Autentisering

Med autentisering menes som regel verifisering av en brukerkonto gjennom passord eller andre mekanismer. En digital identitet kan ha flere brukerkontoer, og tilgang til informasjonssystemer styres som hovedregel gjennom autentiseringen av en brukerkontos passord. I henhold til pasientjournalloven § 22 skal det være tilgangsstyring, logging og etterfølgende kontroll.

Sikkerhetsprinsipper for autentisering	
3.6.1	Autentisering skal gjøres mot sentral autentiseringsløsning.
3.6.2	Passord skal opprettes, lagres, sendes og forvaltes etter regional passordpolitikk.
3.6.3	Systemet skal kunne håndheve passordkompleksitet i henhold til HMNs passordpolitikk.
3.6.4	Autentisering skal ha tilstrekkelig styrke iht. «beste praksis». Styrken på autentiseringen skal avgjøres av anbefalingen fra en risikovurdering av tjenesten. Nasjonale føringer skal legges til grunn[4].
3.6.5	Det skal benyttes to-faktorautentisering, hvorav passord er en av faktorene ved: • Tilgang fra eksterne nettverk (ekstranett, Internett, leverandører) • Tilgang fra klientnettverket mot admin nettverket Styrken på autentiseringen skal avgjøres av anbefalingen fra en risikovurdering av tjenesten. Nasjonale føringer skal legges til grunn[4].
3.6.6	Alle tilgangsforespørsler til integrasjonsgrensesnitt skal autentiseres vha. en internasjonal standard tilsvarende OAuth 2.0
3.6.7	Informasjonssystemer skal støtte Single Sign-On (SSO).
3.6.8	Ansatte i andre virksomheter skal kunne automatisk autentiseres vha. en internasjonal standard og protokoll for sikker utveksling av identiteter mellom ulike organisasjoner tilsvarende OAuth 2.0.

3.7. Autorisering (tilgangsstyring)

Med autorisering menes å gi korrekte tilganger til en autentisert konto. I virksomheten er det som hovedregel katalogtjenesten Active Directory som er autoritativ for rettigheter og tilganger.

Det settes en rekke krav til tilgangsstyring for behandlingsrettede helseregistre. Dette gjelder for både virksomhetsinterne og regionale journalsystemer. I pasientjournalloven §22 står det at den dataansvarlige og databehandleren skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet, herunder oppfyller krav til tilgangsstyring, logging og etterfølgende kontroll.

Pasientjournalloven § 19 stiller krav til at dataansvarlig tilgjengeliggjøre helseopplysninger for helsepersonell og annet samarbeidende helsepersonell når det er nødvendig for å yte, administrere og kvalitetssikre helsehjelpen.

[4] Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor - regjeringen.no

Pasientjournalloven åpner for nye måter å organisere pasientjournaler og tilganger til slike journaler. Det er likevel viktig at kravet om tjenstlig behov til enhver tid opprettholdes. Dette innebærer at løsninger med felles behandlingsrettede helseregistre må kunne ivareta de grunnleggende kravene knyttet til konfidensialitet om pasientenes helseopplysninger.

Sikkerhetsprinsipper for autorisering	
3.7.1	Tilganger skal gis basert på roller.
3.7.2	Tilganger skal gis på et lavest mulig nivå, og basert på tjenstlig behov.
3.7.3	Tilganger skal være tidsbegrenset for innleid personell, og skal ikke overskride innleieavtalens varighet.
3.7.4	Tilganger skal fjernes når formålet opphører.
3.7.5	Tilganger, endringer i tilganger og hvem som beslutter endringer i tilganger skal loggføres.

Spesielt for behandlingsrettede helseregistre	
3.7.6	Behandlingsrettede helseregistre skal støtte attributtbasert tilgangskontroll der attributtene som benyttes til autorisasjon (tilgangskontroll) minimum omfatter ansettelses- eller arbeidsforholdet til brukeren og rollen[5] brukeren har i sitt påloggede arbeidsforhold.
3.7.7	Rollen[6] brukeren har i et behandlingsrettet helseregister skal avgjøre hvilken tilgang brukeren får til informasjonen og applikasjonsfunksjonene i det behandlingsrettede registeret.
3.7.8	Attributtene som følger med identiteten til den ansatte/innleide ved pålogging til et behandlingsrettet helseregister, skal i tillegg kunne avgjøre hvilke tilganger den ansatte har til funksjonene i det behandlingsrettede helseregisteret.
3.7.9	Behandlingsrettede helseregistre skal kunne ha roller som skiller på tilganger basert på • Organisatorisk tilhørighet • Pasienter under aktiv behandling, før aktiv behandling, og etter aktiv behandling • Arbeidsgruppetilhørighet
3.7.10	Virksomheten skal opprette rutiner for tildeling av tilganger i behandlingsrettede helseregistre og stikkprøvekontroll av tilganger.
3.7.11	Rollen[7] den ansatte innehar i et behandlingsrettet helseregister skal skille dennes tilganger til pasienter i aktiv behandling[8] på angitte organisasjonsenheter, fra tilgang i forkant og etterkant av aktiv behandling.

[5] Rollen brukeren har er definert i den regionale rollemodellen f.eks. «lege», «sykepleier», «farmasøyt», osv.
[6] Det forutsettes at den enkelte ansatt/innleide kan ha ulike roller i ulike arbeidsforhold.
[7] Tidsperspektivet må enkelt kunne endres og varieres avhengig av rolle.
[8] Inneliggende og poliklinikk.

3.7.12	Rollen den ansatte innehar i et behandlingsrettet helseregister skal gi mulighet for den ansatte selv til å beslutte tilgang til ikke-aktive[9] pasienter.
3.7.13	Rollen den ansatte innehar i et behandlingsrettet helseregister skal gi mulighet for den ansatte til å beslutte tilgang for en kollega som selv ikke har tilgang til pasienten som ikke er under aktiv behandling.
3.7.14	Rollen den ansatte innehar i et behandlingsrettet helseregister skal gi mulighet for tilgang til pasienter via «arbeidsgruppe» (organisering og gruppering av pasienter uten avhengighet til organisasjonens formelle enheter).
3.7.15	Rollen den ansatte innehar i et behandlingsrettet helseregister skal gi mulighet for å eksplisitt beslutte tilgangen til pasienter begrenset til (skal kunne velge en eller flere kriterier samtidig): • hvilke sett av organisasjonsenheter pasienten tidligere har vært behandlet ved innen et foretak, eller hele foretaket under ett • hvilke sett av organisasjonsenheter pasienten tidligere har vært behandlet ved på tvers av flere foretak, eller inkludert et eller flere hele foretaket • gitte diagnoser/kombinasjoner av diagnoser, eller alle diagnoser • antall måneder/år tilbake i tid for når pasienten ble behandlet av gitt org.enhet • inkluder døde pasienter ja/nei • pasienter i et gitt pasientforløp
3.7.14	Rollen den ansatte innehar i et behandlingsrettet helseregister skal gi mulighet for å delegere pasienter til en eksisterende arbeidsgruppe ut fra følgende utvalgskriterier: • pasienter som har vært behandlet ved gitte sett av organisasjonsenheter innen et foretak, eller hele foretaket under ett • pasienten som har vært behandlet ved gitte sett av organisasjonsenheter på tvers av flere foretak, eller et eller flere foretaket • pasienter med valgt kombinasjon(er) av diagnose- og prosedyrekoder, eller alle diagnoser • antall måneder/år tilbake i tid for når pasienten ble behandlet av gitt org.enhet • inkluder døde pasienter ja/nei • pasienter i et gitt pasientforløp
3.7.15	Det skal være mulig å entydige identifisere hvem som er juridisk[10]- og/eller medisinsk ansvarlig[11] for en gitt pasient innen en juridisk enhet og på tvers av juridiske enheter involvert i pasientens behandling.

[9] Pasienter som ikke har noen aktive forhold til foretak
[10] Med juridisk ansvar menes den organisasjonsenheten som juridisk har ansvaret for pasientens behandling
[11] Med medisinsk ansvar menes den legen eller psykolog som er pasientansvarlig

3.8. Identitets- og tilgangsstyring

Dette kapittelet gjelder kravstilling til applikasjoner som skal benytte identitets- og tilgangsstyring.

Sikkerhetsprinsipper for identitets- og tilgangsstyring	
3.8.1	Applikasjonen bør støtte moderne autentiseringsmekanismer for skytjenester, og herunder benyttelse av multifaktorautentisering (MFA).
3.8.2	Applikasjonen skal støtte anerkjente federeringsteknologistandarder (f.eks. OpenID Connect) som autentiseringsmekanisme.
3.8.3	Ved pålogging til kliniske applikasjoner skal som minimum attributtene brukerID, organisasjonstilknytning og rolle tas imot og behandles for å etablere en sikkerhetssesjon.
3.8.4	Applikasjonen skal håndheve sikkerhetssesjonen. Dette inkluderer, men er ikke begrenset til inaktivitet, start- og sluttidspunkt på token.
3.8.5	Ved behov for ny eksplisitt autentisering (reautentisering og/eller autentisering av annen bruker) skal ny sikkerhetssesjon startes.
3.8.6	Tilgang til funksjonalitet og pasientdata i applikasjonen skal baseres på kombinasjon av brukers rolle og organisasjonstilknytning. I hovedsak gir rolle tilgang til funksjoner mens organisasjon styrer pasienttilgang. Dette støttes ved bruk av interne tilgangskontrollmekanismer og/eller ekstern autoriseringstjeneste.
3.8.7	Applikasjonen skal spørre ekstern autoriseringstjeneste om det finnes en aktiv pasient-behandlerrelasjon dersom intern tilgangskontrollmekanisme ikke kan avgjøre tilgang.
3.8.8	Dersom ekstern autoriseringstjeneste benyttes skal kall mot denne gjøres i henhold til internasjonale autoriseringsstandarder som f.eks. OAuth 2.0.
3.8.9	Applikasjonen skal være i stand til å tilpasse seg Helse Midt-Norges sikkerhetsarkitektur relatert til attributtbasert tilgangskontroll (ABAC).
3.8.10	Ved nektet tilgang bør applikasjonen presentere begrunnelsen på en forståelig måte til sluttbruker.
3.8.11	Applikasjonen skal hver person (identitet) har sin egen entydige regionale bruker-ID.
3.8.12	Applikasjonen bør støtte gruppering av rettigheter ved at roller for tilgang kan defineres og gis rettigheter slik at brukere kan tildeles roller i stedet for individuelle rettigheter.
3.8.13	Applikasjonen skal støtte at det kan være flere roller og/eller organisasjoner knyttet til samme entydige bruker-ID.
3.8.14	Applikasjonen skal støtte unik identifikator for entydig identifikasjon av organisasjonsenheter.
3.8.15	Leverandøren skal tilpasse sitt produkt slik at tilganger kan differensieres på hvor den ansatte jobber til enhver tid.
3.8.16	Applikasjonen skal støtte provisjonering (oppretting, lesing, endring og sletting) via standardisert programmeringsgrensesnitt (API). Programmeringsgrensesnittet skal:

	• Være tydelig dokumentert • Ha standardisert autentiseringsmekanisme • Benytte kryptert kommunikasjon • Kommunisere over HTTPS, LDAPS eller SQL over TLS Programmeringsgrensesnittet bør: • Være REST-API over HTTPS tilnærmet SCIM-standarden
3.8.17	APIet skal muliggjøre provisjonering av påloggingsklare brukere med forhåndsdefinerte standardtilganger uten behov for manuelle tilleggsoperasjoner.
3.8.18	APIet bør muliggjøre tildeling av individuelle rettigheter i tillegg til standardtilganger.
3.8.19	Applikasjonen bør tilby et brukergrensesnitt for brukeradministrasjon, i tillegg til APIet.
3.8.20	APIet skal muliggjøre uthenting av eksisterende data knyttet til bruker, rolle, organisasjon og tilganger fra applikasjonen.

3.9. Sperring

Den enkelte pasient skal kunne motsette seg at helseopplysninger blir brukt i den videre behandling av pasienten (rett til sperring). Behandlingsrettede helseregistre må dermed ha støtte for å sperre tilgang til helseopplysninger for en valgt pasient. Sperrede opplysninger skal kunne åpnes enten etter pasientens eget ønske eller dersom behandler vurderer at det foreligger "tungtveiende grunner" etter pasient- og brukerrettighetsloven § 5-3.

I Pasientjournalloven § 7 må behandlingsrettede helseregistre være utformet slik at det oppfyller pasientens rett til å motsette seg behandling av helseopplysninger.

Manuell støtte i forkant for sperring:

- Journalansvarlig skal forklare pasienten konsekvensen ved sperring, og at det eventuelt kan ha betydning for videre helsehjelp. Dersom pasienten er samtykkekompetent, og har fått forklart konsekvensene, skal pasientens krav om sperring etterkommes. Journalansvarlig er person som omtalt i helsepersonelloven § 39 andre ledd. Journalansvarlig skal være oppnevnt, og har ansvar for innhold av journal, og vil normalt være den som må vurdere krav om retting, sletting og sperring.
- Dersom ikke kravet etterkommes, skal det sendes informasjon til pasienten om retten til å klage til helsetilsynet i fylket.

Behandlingsrettede helseregistre må derfor understøtte at pasienten kan detaljere hvem som ikke skal kunne ha tilgang i sin journal og hvilken informasjon det skal begrenses innsyn i.
Tabellen under gir kravene til slik sperring. Kravene gjelder både internt i et helseforetak og mellom helseforetak. Kravene skal anvendes både på eksisterende informasjon og dokumenter og framtidig informasjon og dokumenter som skal etableres.

Spesielt for behandlingsrettede helseregistre	
3.9.1	Det skal være mulig i et behandlingsrettet helseregister etter forespørsel fra en pasient å begrense tilgangen til journalen til en pasient, slik at en navngitt person, eksempelvis nabo eller nær slektning, ikke skal ha tilgang til hele eller utvalgte deler av journalen til pasienten.
3.9.2	Det skal være mulig i et behandlingsrettet helseregister etter forespørsel fra en pasient å begrense tilgangen til journalen til en pasient, slik at utelukkende enkeltpersoner eller enkeltpersoner i en gitt rolle, eksempelvis alle leger, skal ha tilgang til journalen til pasienten, og dermed sperre tilgangen for alle andre.
3.9.3	Det skal være mulig i et behandlingsrettet helseregister etter forespørsel fra en pasient å begrense tilgangen til journalen til en pasient, slik at kun ansatte som tilhører en eller flere organisasjonsenheter, eksempelvis avdeling på et lokalsykehus, skal ha tilgang til journalen til pasienten, og dermed sperre tilgangen for alle andre brukerne.
3.9.4	Kriteriene i krav 4.9.2 og 4.9.3 skal kunne kombineres for å definere hvem som skal gis tilgang til journalen til en pasient, og dermed sperre tilgang for alle andre.
3.9.5	Det skal være mulig i et behandlingsrettet helseregister etter forespørsel fra en pasient å begrense tilgangen til journalen til pasienten, slik at alle enkeltpersoner eller enkeltpersoner i en gitt rolle, eksempelvis sykepleier eller fysioterapeut, ikke skal ha tilgang til journalen til pasienten, og dermed sperre tilgangen for disse brukerne.
3.9.6	Det skal være mulig i et behandlingsrettet helseregister etter forespørsel fra en pasient å begrense tilgangen til journalen til pasienten, slik at ansatte tilhørende en eller flere organisasjonsenheter, eksempelvis en avdeling, lokalsykehus eller foretak, ikke skal ha tilgang til journalen til pasienten, og dermed sperre tilgangen for disse brukerne.
3.9.7	Kriteriene i krav 4.9.5 og 4.9.6 skal kunne kombineres for å definere hvem som ikke skal gis tilgang til journalen til en pasient.
3.9.8	Det skal være mulig i et behandlingsrettet helseregister etter forespørsel fra en pasient å sperre tilgangen for en periode, inkludert på ubestemt tid fremover, til enkelte dokumenter i journalen. Kravet skal kunne gjennomføres på dokumenter sperret etter alle kriteriene angitt, ref. kravsettene angitt under 4.9.1-4.9.7.
3.9.9	Det skal være mulig i et behandlingsrettet helseregister etter forespørsel fra en pasient å sperre tilgangen for en periode, inkludert på ubestemt tid fremover, til enkelte dokumenttyper som vil bli opprettet i journalen. Kravet skal kunne gjennomføres på dokumenter sperret etter alle kriteriene angitt, ref. kravsettene angitt under 4.9.1-4.9.7.
3.9.10	Det skal være mulig i et behandlingsrettet helseregister etter forespørsel fra en pasient å sperre tilgangen for alle dokumenter som er opprettet i en definert periode i journalen.
3.9.11	Det skal være mulig i et behandlingsrettet helseregister etter forespørsel fra en pasient kun å gi tilgang for alle dokumenter som er opprettet i en definert periode i journalen.

3.10. Ikke-benekt (digital signering med sertifikat)

Spesielt for behandlingsrettede helseregistre	
3.10.1	Avsender bør kunne digitalt signere utvalgte dokumenter med kvalifisert sertifikat.

3.11. Sporbarhet

Med sporbarhet menes å kunne bevare nødvendige detaljer knyttet til en handling, herunder uavviselighet. Uavviselighet, eller ikke-benekting, er å bekrefte at en handling eller et informasjonselement er uendret, og at det entydig kan knyttes til en bestemt digital identitet. Dette benyttes også i sammenheng med autorisering og autentisering.

Dataansvarlig og databehandler skal sørge for tilgangsstyring, logging og etterfølgende kontroll i behandlingsrettede helseregister. Bruk av informasjonssystem skal dokumenteres. Dette følger av pasientjournalloven § 22 og pasientjournalforskriften § 14. Det stilles videre krav om at loggene skal kontrolleres.

Det følger av pasientjournalloven § 18 at pasienten eller brukeren har krav på informasjon og innsyn i behandlingsrettede helseregistre. Dette omfatter også innsyn i hvem som har fått tilgang til eller utlevert helseopplysninger om vedkomne. Behandlingsrettede helseregistre må derfor understøtte krav om sporbarhet på hvem som har fått tilgang til eller utlevert helseopplysninger.

Sikkerhetsprinsipper for sporbarhet	
3.11.1	Alle handlinger som kan ha betydning for informasjonssikkerheten i systemet skal logges. Dette inkluderer, men er ikke begrenset til: • Alle typer innlogginger, inkl. forsøk på innlogginger • Oppretting, endring og sletting av informasjonsobjekter • Oppretting, endring og sletting av andre brukere • Innsyn eller endring i helseopplysninger • Endringer, eller forsøk på endringer, i systemkonfigurasjonen • Sikkerhetseventer[12], avvik og fravik
3.11.2	Endringer i en tjeneste skal dokumenteres i systemdokumentasjonen, og endringer som påvirker informasjonssikkerheten skal risikovurderes.
3.11.3	Logging skal legge til rette for at helseforetakene kan avdekke sikkerhetsbrudd og forsøk på misbruk skal kunne oppdages.
3.11.4	Logger skal tilgangsstyres slikt at de beskyttes mot manipulering/endring.
3.11.5	Logger skal ha tidsstempling og være synkronisert mot intern NTP-server.
3.11.6	Logger som er relevante for informasjonssikkerheten skal kunne overføres til sentralt loggmottak.

[12] En sikkerhetsevent er identifisert tilfelle av en tilstand i system, tjeneste eller nettverk som idikerer et mulig brudd på informasjonssikkerhetspolicy, avvik fra kontroller eller en tidligere ukjent situasjon som kan være relevant for informasjonssikkerheten.

3.11.7	Logger skal gjennomgås manuelt eller automatisk basert på forhåndsdefinerte kriterier.
3.11.8	Logger skal oppbevares i tråd med krav fastsatt i lov eller avtale. Logger av sikkerhetsmessig betydning bør oppbevares så lenge som nødvendig for å oppnå formålet. Pasientjournallogger og andre logger knyttet til behandlingsrettede registre, skal lagres like lenge som journalen loggen er knyttet til.

Spesielt for behandlingsrettede helseregistre[13]	
3.11.9	Følgende skal 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 I dette ligger at som minimum skal følgende konkrete aktiviteter logges: • pålogging • utlogging • åpning av pasientjournal • lesing i pasientjournal • skriving i pasientjournal • sletting av opplysninger i pasientjournal • sperring av pasientjournal • fletting • utskrift • oppretting og endring av tilganger og rettigheter • kopiering og sletting av brukerroller • eksport av datasett • søk som er gjort
3.11.10	Følgende informasjon skal minimum lagres ved tilgang og aktivitet i et behandlingsrettet helseregister: • Identiteten og rollen til den som har lest, rettet, registrert, endret og/eller slettet helse- og personopplysninger • Organisatorisk tilhørighet • virksomhetstilhørighet • Grunnlaget for tilgjengeliggjøringen • Tidsperioden for tilgjengeliggjøringen

[13] Behandlingsrettede helseregistre skal oppfylle kravene under, i tillegg til kravene i punkt 11.1-11.8. Krav 11.9-11.12 gjelder ikke for systemer som ikke ansees å være behandlingsrettede helseregistre.

3.11.11	Det skal være mulig manuelt og automatisert å hente ut loggdata fra behandlingsrettede helseregistre.
3.11.12	Tjenestekonsumenter fra andre juridiske enheter som bruker delsystemene i løsningen, skal kunne spores i regional klinisk løsning, samt i den plattformen og de infrastrukturtjenester som utgjør sikkerhetsarkitekturen.

3.12. Serversikkerhet

Med serversikkerhet menes de tiltakene som er implementert for å oppnå akseptabel risiko for servere[14].

Sikkerhetsprinsipper for serversikkerhet	
3.12.1	Servere skal som minimum herdes i tråd med instruks fra Hemit. Ved konflikt i kravsett mellom applikasjonsleverandør og instruks fra Hemit, skal det gjennomføres risikovurdering.
3.12.2	Serveren skal ha installert gjeldende sikkerhetsoppdateringer og antivirussignaturer innen rimelig tid[15] iht. kritikalitet.
3.12.3	Serveren skal inngå i driftsovervåkingen.
3.12.4	Servere skal ha identifiserte krav for: • Back-up • Patching • Tilgjengelighet, inkludert: - Feilrettingstid - Redundans og geo-redundans
3.12.5	Serveren skal synkronisere klokken mot intern NTP-server.
3.12.6	Serveren skal avgi logger til sentralt loggmottak.
3.12.7	Bruk av ressurser skal inn i regime for overvåking og justering, og det bør foretas beregninger over framtidige kapasitetsbehov for å sikre at systemet oppnår påkrevd ytelse.

3.13. Klientsikkerhet

Med klientsikkerhet menes de tiltakene som er implementert for å oppnå akseptabel risiko for klienter.

Sikkerhetsprinsipper for klientsikkerhet	
3.13.1	Klienter skal ha kryptert harddisk.
3.13.2	Klienter skal ha automatisk installasjon av sikkerhetsoppdateringer og antivirussignaturer.

[14] Server: inkludert appliance-enheter og terminalservere. Virtual Desktop Interface (VDI) går som klient og ikke server.
[15] I vurderingen av hva som ansees som «rimelig tid» må det også sees hen til anbefalinger fra offentlige CERT og lignende.

3.13.3	Klienter skal ha automatisk låsing av skjerm m/ passord[16].
3.13.4	Klienter skal være innkjøpt, forvaltet, konfigurert og godkjent av Hemit. Klienter som ikke eies av Hemit skal heller ikke kunne kobles til virksomhetens nettverk uten at det foreligger en godkjent risikovurdering (gjelder ikke gjestenettverk).
3.13.5	Brukere skal ikke ha administrasjonsprivilegier på egen klient. Brukere skal ikke kunne deaktivere lokale sikkerhetskontroller
3.13.6	Klienter skal kun ha godkjent programvare installert.
3.13.7	Klienter skal alltid benytte VPN eller tilsvarende teknologi når man er utenfor HMNs infrastruktur, for eksempel private eller offentlige nettverk.
3.13.8	Klienter skal autentiseres gjennom klientsertifikater for å kunne koble seg på HMNs nettverk.

3.14. Applikasjonssikkerhet

Med applikasjonssikkerhet menes sikkerhet i de tjenestene som benyttes for å utføre databehandlingen.

Sikkerhetsprinsipper for applikasjonssikkerhet	
3.14.1	Applikasjoner som behandler skjermingsverdig informasjon skal ha egen tilgangskontroll med autentisering og autorisering mot sentral tjeneste. Andre applikasjoner bør ha egen tilgangskontroll med autentisering og autorisering mot sentral tjeneste.
3.14.2	Relevante applikasjoner skal avgi nødvendige sikkerhetslogger til sentralt loggmottak.
3.14.4	Applikasjonen skal styres gjennom Hemits applikasjonsforvaltning.
3.14.5	Det skal legges til rette for effektiv og hurtig installasjon av sikkerhetsoppdateringer. Om nødvendig skal det opprettes eget testmiljø for å verifisere oppdateringene.
3.14.6	Applikasjoner som behandler helseopplysninger skal benytte en trelagsarkitektur for å begrense eksponering av bakenforliggende database.
3.14.7	Applikasjonen skal kryptere data som går i transitt utenfor vår fysiske kontroll.

3.15. Administrasjon

Med administrasjon menes den driftsoppgaven som må utføres for at IKT-utstyr og tjenester skal fungere i tråd med hensikt og formål.

Sikkerhetsprinsipper for administrasjon	
3.15.1	Administrasjon av servere og tjenester skal gjøres gjennom et eget administrasjonsnettverk.

[16] Gjelder ikke for PULS Spesial

3.15.2	Administrasjon av servere og tjenester skal gjøres av autorisert personell, med tilhørende personlige administratorbrukere.
3.15.3	Det skal benyttes to-faktorautentisering for å koble til administrasjonsnettverket.
3.15.4	Administrasjonsnettverket skal ikke ha tilgang til Internett eller andre eksterne nettverk.
3.15.5	Servere i administrasjonsnettverket skal sikkerhetsoppdateres oftere eller minimum minst like ofte som vanlig produksjonsutstyr.
3.15.6	Servere i administrasjonsnettverket skal avgi logger til sentralt loggmottak på lik linje som vanlig produksjonsutstyr.
3.15.7	Utveksling av informasjon og programvare mellom virksomheter skal baseres på en formell utvekslingspolicy, gjennomført i henhold til utvekslingsavtaler, og skal være i samsvar med all relevant lovgivning.
3.15.8	Det skal benyttes egne Management Workstations ved administrering av servere i HMN og kundedomener.

3.16. Avhending

Med avhending menes at IKT-utstyr må skiftes ut. Dette innebærer at IKT-utstyret ikke lenger vil inngå i informasjonsbehandlingen i virksomheten, og skal enten destrueres, resirkuleres, selges, leveres tilbake til leasing-leverandør, gis bort eller på annen måte avslutte det juridiske eierskapet hos virksomheten.

Sikkerhetsprinsipper for avhending	
3.16.1	Avhending av IKT-utstyr som inneholder helse- eller personopplysninger skal alltid sikres mot uautorisert innsyn og gjøres slik at innholdet garantert ikke kan gjenskapes.
3.16.2	Lagringsmedium som inneholder helse- eller personopplysninger, selv om disse er kryptert, skal merkes på en tilstrekkelig måte.
3.16.3	Avhending til tredjepart skal ikke gjennomføres før det foreligger godkjent risikovurdering og signert databehandleravtale.

3.17. Leverandører og annet eksternt personell

Med leverandører menes ekstern tredjepart som utfører databehandling, vedlikehold, service, drift, forvaltning eller lignende på vegne av virksomheten. Dette gjelder både for fysisk oppmøte og fjernaksess.

Sikkerhetsprinsipper for leverandører	
3.17.1	Leverandøren skal forsikre at de har rutiner som pålegger alle medarbeidere taushetsplikt om helse- og personopplysninger og annen taushetsbelagt informasjon. Leverandøren kan selv administrere og oppbevare taushetserklæringer for eget personell, men den dataansvarlige skal sikres innsyn ved behov.

3.17.2	Alle leverandører som utfører databehandling på vegne av helseforetakene i Helse Midt-Norge, eller arbeid hvor innsyn i helse- og personopplysninger er jevnlig forventet å forekomme, skal signere databehandleravtale.
3.17.3	Alle leverandører som skal behandle helse- og personopplysninger skal kunne dokumentere egen informasjonssikkerhet.
3.17.4	All leverandørtilgang over fjernaksess skal gjøres gjennom Hemits leverandørportal.
3.17.5	Leverandører skal ikke gis administratortilgang til IKT-utstyr i virksomhetenes nettverk, uten at det foreligger en godkjent risikovurdering.
3.17.6	Leverandører skal ikke flytte eller kopiere data ut fra IKT-utstyr i virksomhetenes nettverk, uten at det foreligger en godkjent risikovurdering.
3.17.7	Når leverandører gis tilgang skal det etableres tekniske barrierer som hindrer leverandøren i å få tilgang til annet enn hva som er formålet med tilgangen.

3.18. Datakommunikasjon

Med datakommunikasjon menes flytting eller kopiering av data mellom noder i Helse Midt-Norge sitt nettverk. Det er Hemit som skal etablere og drifte logiske og fysiske nettverk i Helse Midt-Norge.

Sikkerhetsprinsipper for datakommunikasjon	
3.18.1	Hemit har ansvar for etablering, drift og kontroll av fysiske og logiske nettverk i Helse Midt-Norge.
3.18.2	Helse Midt-Norge sitt fysiske nettverk skal logisk oppdeles for å understøtte god informasjonssikkerhet.
3.18.3	Løsninger med behov for datakommunikasjon bør støtte mikrosegmentering.
3.18.4	Åpninger mellom logiske nettverk skal kun skje etter særskilt vurdering av risikoen.
3.18.5	Fysiske eller logiske nettverk som ikke kontrolleres av Hemit, anses å være ekstranettverk. Ekstranett og andre eksterne nettverk skal sammenkobles gjennom Helse Midt-Norge WAN-mottak. Lokale VPN-forbindelser mv. mot ekstranett eller tredjepart er ikke tillatt.
3.18.6	Alt utstyr som skal bruke nettverket og kommunisere over nett skal bruke kryptert kommunikasjon med sikre passord.

3.19. Sonemodell

Med sonemodell menes arkitekturbeslutningen hvor Helse Midt-Norge har etablert en sonemodell basert på fire sikkerhetsnivåer.

Sikkerhetsprinsipper for sonemodell	
3.19.1	Kommunikasjon skal alltid initieres av tjenesten i det høyeste sikkerhetsnivået.
3.19.2	Informasjon som går mellom sikkerhetsnivåer skal alltid avidentifiseres/filtreres før informasjonen forlater sitt opprinnelige sikkerhetsnivå.
3.19.3	Brannmur skal ikke åpnes med mindre det foreligger godkjent løsningsdesign.

3.19.4	Informasjon som hentes fra en lavere sikkerhetskontekst skal alltid kontrolleres for ondsinnet kode eller tilsvarende.

3.20. Angrepsflate

Med angrepsflate menes summen av de tjenester og servere som virksomheten eksponerer mot Internett og som dermed utgjør virksomhetens digitale fotspor.

Sikkerhetsprinsipper for angrepsflate	
3.20.1	Angrepsflaten skal begrenses til et minimum.
3.20.2	Alle tjenester som eksponeres eksternt skal penetrasjonstestes, uavhengig av sikkerhetsnivå.
3.20.3	Alle tjenester som eksponeres eksternt skal plasseres i virksomhetens DMZ.
3.20.4	Kompromitterte tjenester i DMZ skal ikke kunne benyttes til å gjennomføre angrep mot bakenforliggende systemer.
3.20.5	En ekstern klient skal aldri kunne sende datapakker inn i systemer bak DMZ.

3.21. Dynamisk utskrift

Dynamisk utskrift er HMNs løsning for utskrift.

Sikkerhetsprinsipper for dynamisk utskrift	
3.21.1	Enheter av typen multifunksjonsprinter (MFP) skal være koblet opp mot dynamisk utskrift.
3.21.2	Enheter som kan skrive ut skal stå i et eget VLAN.
3.21.3	Enheter som bruker dynamisk utskrift skal ha automatisk utlogging etter bruk eller inaktivitet.
3.21.4	Enheter skal være forvaltet, konfigurert og godkjent av Hemit.
3.21.5	Brukere skal ikke ha administrasjonsprivilegier på utskriftsenheter. Brukere skal ikke kunne deaktivere lokale sikkerhetsfunksjoner på disse enhetene.
3.21.6	Applikasjoner skal støtte utskrift via dynamisk utskrift.

3.22. Dokumentasjon

Sikkerhetsprinsipper for dokumentasjon	
3.22.1	Virksomheten skal dokumentere informasjonssystemene sine, inkl. konfigurasjon, endringer og rutiner for bruk av systemet/løsningen
3.22.2	Systemdokumentasjon skal være lagret og holdes oppdatert på godkjent område for oppbevaring i minst fem år etter siste endring.
3.22.3	Det skal være opprettet planer for business continuity og disaster recovery for systemet.

3.23. Publikumstjenester

Hvis tjenesten regnes som en publikumstjeneste skal tabellen under fylles ut.

Sikkerhetsprinsipper for publikumstjenester	
3.23.1	Publikumstjenester skal settes opp på eget separat nettverk.
3.23.2	Datatilsynets retningslinjer for bruk av informasjonskapsler[17] skal følges.
3.23.3	Tjenesten skal følge lovkrav[18] til universell utforming av IKT.
3.23.4	Alle eksterne nettsteder driftet av virksomheten, som har informasjon annet enn kontekst 1 – Åpen, inkludert alle sider som har noen form for pålogging, skal være utstyrt med digitalt sertifikat, og konfigurert for sikker kommunikasjon.

3.24. Terminering av eksisterende tjenester

Hvis tjenesten erstatter eller fører til nedstenging av eksisterende tjeneste skal tabellen under fylles ut.

Stenging av eksisterende tjeneste	
3.24.1	Eksisterende utstyr er avhendet forsvarlig.
3.24.2	Brannmursåpninger er lukket.
3.24.3	System- eller administratorkontoer er fjernet.
3.24.4	Systemet er markert som inaktivt i tjenestekatalogen.

4. Avvik

Avvik på denne instruks meldes i virksomhetens avvikssystem. Informasjonssikkerhetsleder og/eller personvernombud skal varsles.

5. Referanser

- Pasientjournalloven
- Personopplysningsloven med tilhørende personvernforordning
- Øvrige dokumenter i styringssystemet
- Regional passordpolitikk

[17] Bruk av informasjonskapsler (cookies) | Datatilsynet
[18] Eksempelvis Forskrift om IKT-standarder i helse- og omsorgstjenesten - Lovdata