Veileder for tilgangsstyring

Veilederen er et støttedokument til Norm for informasjonssikkerhet

Utgitt med støtte av:

Direktoratet for e-helse

Versjon 1.0

www.normen.no

Merknad 24.03.2019: Dokumentet er ikke oppdatert fra siste versjon av Normen (5.3), ny personopplysningslov, endringer i helselovgivningen, eller EUs personvernforordning

INNHOLD

1 INNLEDNING 4

1.1 BAKGRUNN 4
1.2 OM VEILEDEREN 4
1.3 MÅLGRUPPE 5
1.4 VEILEDERENS FORHOLD TIL EUS NYE PERSONVERNFORORDNING 6

2 LOVGRUNNLAG 7

3 TILGANGSSTYRING 9

3.1 PERSONALADMINISTRASJON I STORE VIRKSOMHETER 10
3.2 RELEVANTE OG NØDVENDIGE HELSEOPPLYSNINGER 10
3.3 AUTORISASJON FOR TILGANG 11
3.3.1 Sperring 11
3.3.2 Rolle 12
3.3.3 Rollemal 12
3.3.4 Tilgang 12
3.3.4.1 Ytelse av helsehjelp 13
3.3.4.2 Tilgangsstyring i små virksomheter 13
3.3.4.3 Beslutningsstyrt tilgang 14
3.3.4.4 Kortvarig tilgang 14
3.3.4.5 Tilgang mellom virksomheter 14
3.3.4.6 Samarbeide om behandlingsrettede helseregistre 16
3.3.4.7 Administrasjon av helsehjelp 16
3.3.4.8 IKT-personell 16
3.3.4.9 Annen hjemmel for tilgang 17
3.3.5 Selvautorisering 17
3.3.6 Autorisasjonsregister 18
3.3.7 Fjerne og endre autorisasjon for tilgang 19
3.4 AUTENTISERING 19
3.4.1 Tildeling av autentiseringskriterier 19
3.4.2 Flere roller 20
3.4.3 Flere ansettelsesforhold 20
3.4.4 Styrken på autentiseringen 20
3.4.5 Internt i virksomheten 21
3.4.6 Portalløsning og skyløsning 21
3.4.7 Tilgang mellom virksomheter 21
3.4.8 Samarbeid om behandlingsrettede helseregistre 22
3.5 KONTROLL AV TILGANGER 22
3.5.1 Tildelte autorisasjoner for tilgang 22
3.5.2 Logger 22

4 EKSEMPLER PÅ PROSEDYRER 23

4.1 TILDELING AV AUTORISASJON FOR TILGANG 23
4.2 KONTROLL AV TILDELTE AUTORISASJONER FOR TILGANG 24
4.3 SELVAUTORISERING - LOGGING OG OPPFØLGING AV LOGGER 25

5 VEDLEGG 26

5.1 ANBEFALTE DOKUMENTER IFM. INFORMASJONSSIKKERHET 26
5.2 DEFINISJONER 26
5.3 REFERANSER 30
5.4 DELTAGERE I REFERANSEGRUPPEN 30

Endringshistorikk for og godkjenning av dokumentet

Versjon	Endringer	Godkjent av styringsgruppen for Normen (dato)
1.0	Første versjon av veilederen	8. juni 2017

1 INNLEDNING

1.1 Bakgrunn

Virksomheter som yter helsehjelp har ansvar for at *behandling* av *helse- og personopplysninger* skjer på en måte som ivaretar *taushetsplikten* og sikrer *pasientenes* personvern, samtidig som opplysningene skal være tilgjengelige for personell ved *virksomheten* som trenger det. Det er kun personell ved *virksomheten* som har *tjenstlig behov* som skal ha *tilgang* til taushetsbelagt informasjon, og de skal ikke få *tilgang* til flere opplysninger enn det som er relevant og nødvendig for å kunne utføre sine oppgaver.

Tilgangsstyringen er ett av flere virkemidler for å gi personell[1] *tilgang* til *helseopplysninger* ut fra *tjenstlig behov* og samtidig hindre uautorisert bruk og uberettiget innsyn i opplysninger. Tilgangsstyring skal gi kontroll på *tilgangen* ved hjelp av *logging*, pasientens rett til innsyn i logger, analyse av logger og oppfølging av mulige sikkerhetsbrudd.

Det er viktig å presisere at personell skal gis *tilgang* til de opplysningene som er relevante og nødvendige for å kunne gjennomføre formålet, som er å yte, administrere og kvalitetssikre helsehjelp.

Tilgang i forbindelse med kvalitetssikring og administrative oppgaver skal også besluttes ut fra *tjenstlig behov*.

1.2 Om veilederen

Veilederen gir veiledning til etterlevelse av kravene i Normen til etablering av tilgangsstyring. Alle kursiverte ord er definert, se kapittel 5.2.

Veilederen gir hjelp til bl.a.:
- Få oversikt over regler for tilgangsstyring
- Forstå prinsipper for *autorisering* for *tilgang*
- Forstå prinsipper for *autentisering*
- Beslutte tilstrekkelig styrke på tilgangsstyringen ift *behandlingen* av *helseopplysninger*
- Å definere *roller* og *rollemaler*

Tabellen nedenfor gir leseveiledning for *virksomheter* ift hvilke kapitler i veilederen som er mest relevant:

Kapittel	Relevant for type virksomhet		
	Store	Mindre	Små
2 Lovgrunnlag	x	x	x
3 Tilgangsstyring	x	x	x
3.1 Personaladministrasjon i store virksomheter	x		
3.3 Autorisasjon for tilgang	x	x	x
3.3.1 Sperring	x	x	x

[1] I denne veilederen benyttes begrepet personell som dekker helsepersonell, administrativt personell, tilsynsaktører og andre som yter tjenester til pasient/bruker

Kapittel	Relevant for type virksomhet		
	Store	Mindre	Små
3.3.2 Rolle	x	x	x
3.3.3 Rollemal	x	x	
3.3.4 Tilgang	x	x	x
3.3.4.2 Tilgangsstyring i små virksomheter			x
3.3.4.3 Beslutningsstyrt tilgang	x	x	
3.3.4.4 Kortvarig tilgang	x	x	
3.3.4.5 Tilgang mellom virksomheter	x	x	
3.3.4.6 Samarbeide om behandlingsrettede helseregistre	x		x
3.3.4.1 Ytelse av helsehjelp	x	x	x
3.3.4.7 Administrasjon av helsehjelp	x	x	
3.3.4.8 IKT-personell	x	x	
3.3.4.9 Annen hjemmel for tilgang	x		
3.3.5 Selvautorisering	x	x	
3.3.6 Autorisasjonsregister	x	x	x
3.3.7 Fjerne og endre autorisasjon for tilgang	x	x	x
3.4 Autentisering			
3.4.1 Tildeling av autentiseringskriterier	x	x	x
3.4.2 Flere roller	x	x	
3.4.3 Flere ansettelsesforhold	x	x	
3.4.4 Styrken på autentisering	x	x	
3.4.5 Internt i virksomheten	x	x	x
3.4.6 Portalløsning og skyløsning	x	x	
3.4.7 Tilgang mellom virksomheter	x		
3.4.8 Samarbeid om behandlingsrettede helseregistre	x		x
3.5 Kontroll av tilganger			
3.5.1 Tildelte autorisasjoner for tilgang	x	x	x
3.5.2 Logger	x	x	x

Veilederen dekker ikke:
- Hva logger skal inneholde
- Detaljert analyse av logger, men bruk av logger ifm kontroll av *tilganger*
- Tilgangsstyring i kjernejournal

1.3 Målgruppe

Målgruppen er *virksomheter* som omfattes av *Normen* og som skal etablere tilgangsstyring iht kravene i *Normen.*

Aktuelle målgrupper er for eksempel:
- *Databehandlingsansvarlig*
- Prosjektleder i forskningsprosjekter
- Sikkerhetsleder
- IKT-ansvarlig
- Databehandler
- Personvernombud

Veilederen vil også være nyttig for *leverandører* av journalsystemer og *fagsystemer*.

1.4 Veilederens forhold til EUs nye personvernforordning

EUs nye personvernforordning vil innføres i norsk lov i mai 2018. Dette vil medføre endringer i den norske personvernlovgivningen og dermed endringer i kravene til den behandling av helse – og personopplysninger som denne veilederen omtaler.

Denne veilederen forholder seg til kravene som følger av dagens personvern- og helselovgivning. Når det er klart hva konsekvensene av den nye personvernforordningen blir for denne veilederen vil den oppdateres med de nye kravene.

Oppdatert informasjon om personvernforordningen fins på:

- Datatilsynet side: https://datatilsynet.no/Regelverk/EUs-personvernforordning/
- KMDs side: https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/nye-personvernregler-i-eu/id2340094/
- Eu's side: http://www.eugdpr.org/

2 LOVGRUNNLAG

Enhver som *behandler* helseopplysninger som er omfattet av pasientjournalloven eller helseregisterloven har *taushetsplikt*.

Taushetsplikten er regulert i helsepersonelloven §§ 21 flg. Pasientjournalloven § 15 og helseregisterloven § 17 henviser til denne. *Taushetsplikten* gjelder for alle som får adgang eller kjennskap til *helseopplysninger*, uavhengig av hvilken rolle vedkommende har ift pasienten og for hvilket formål opplysningene *behandles*.

Utgangspunktet er at personell har *taushetsplikt* om det de får kjennskap til om *pasientene* under utøvelsen av sitt yrke. Det gjelder både opplysninger om helseforhold og andre personlige forhold. *Taushetsplikten* innebærer både en passiv plikt til å tie og en aktiv plikt til å hindre at uvedkommende får *tilgang* til taushetsbelagt informasjon. For å utlevere eller gi *tilgang* til helseopplysninger må man ha hjemmel i lovverket. Etter helsepersonelloven § 25 kan man gi opplysninger til personell som samarbeider om å yte helsehjelp til en *pasient*. Helsepersonelloven § 45 gir hjemmel til å utlevere nødvendige og relevante opplysninger til annet helsepersonell som skal yte helsehjelp til *pasienten*. Helsepersonelloven § 25 regulerer de situasjonene hvor helsepersonell samarbeider om helsehjelpen til en *pasient* uavhengig av om dette skjer innenfor eller på tvers av *virksomheter*, mens helsepersonelloven § 45 regulerer plikten til å gi helseopplysninger til andre som yter eller skal yte helsehjelp til samme *pasient* (dvs. utenfor samarbeidssituasjonene). Både helsepersonelloven § 25 og § 45 forutsetter imidlertid at *pasienten* ikke motsetter seg at opplysningene deles eller utleveres. Et system for tilgangsstyring må i ivareta lovens krav til overholdelse av *taushetsplikten*, unntak fra *taushetsplikten*, og pasientens krav om sperring av opplysninger. Det vises til rundskriv IS-8/2012 «Helsepersonelloven med kommentarer» for utdypende informasjon om disse bestemmelsene.

Pasientjournallovens § 19 pålegger virksomheter å sørge for at *helseopplysninger* er tilgjengelige for helsepersonell og annet samarbeidende personell når det er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp, innenfor rammene av *taushetsplikten*. Utfordringen for *virksomheter* som yter helse- og omsorgstjenester er å organisere *virksomheten* slikt at *taushetsplikten* ivaretas samtidig som det legges til rette for deling av pasientopplysninger i gitte tilfeller. I tillegg skal *virksomheten* påse at det ikke deles opplysninger i strid med pasientens ønske. Alle disse forutsetningene og flere, ligger til grunn for de krav som stilles til behandlingsrettede helseregistre i pasientjournalloven § 7 og til helseregistre i helseregisterloven § 6.

Tilgangsstyring er et viktig verktøy som skal sikre at *tilgang* til *helseopplysninger* kun gis til autorisert personell ved *tjenstlig behov*. Mangelfull tilgangsstyring vil være i strid med *virksomhetens* plikt til å sikre at *taushetsplikten* ivaretas og kan også være i strid med *virksomhetens* plikt til å sørge for at nødvendige *helseopplysninger* er tilgjengelige. Ved hjelp av riktig tilgangsstyring kan pasientopplysninger gjøres tilgjengelig for den som har tjenstlig behov for *tilgang* samtidig som opplysningene er utilgjengelige for andre – innenfor samme *virksomhet*. Ved tjenstlig behov skal *tilgangen* som gis begrenses til det som er nødvendig og relevant, jf. helsepersonelloven §§ 25 og 45, pasientjournalloven §§ 16 og 19, helseregisterloven § 18 og forskrift om *tilgang* mellom virksomheter § 6 b).

En rekke lover og forskrifter stiller konkrete krav om at den *databehandlingsansvarlige* skal sørge for tilfredsstillende tilgangsstyring. Pasientjournalloven § 22, første ledd, stiller krav til sikring av *konfidensialitet*, *integritet* og *tilgjengelighet*, dvs. *tilgang* til korrekte opplysninger, til autoriserte personer ved *tjenstlig behov*. Denne plikten omfatter bl.a. å sørge for tilgangsstyring, logging og etterfølgende kontroll. Helseregisterloven § 21 er likelydende mens personopplysningslovens § 13 stiller overordnete krav til sikring av konfidensialitet, integritet og tilgjengelighet. Personopplysningsforskriftens §§ 2-8 til 2-14 stiller ytterligere krav om hvordan dette skal oppnås.

Forskrift om *tilgang* mellom virksomheter, § 7, stiller konkrete krav til tilgangsstyring ved *tilgang* mellom *virksomheter*. Den pålegger begge *virksomhetene* å ha på plass løsninger som ivaretar at opplysningene ikke gjøres tilgjengelige dersom pasienten har motsatt seg slik *tilgang*, at *tilgangen* begrenses til det som er nødvendig og relevant for formålet, at helsepersonell er *autorisert* for *tilgang* og *autentiseres* ved bruk av sikker autentiseringsløsning.

Pasientens rettigheter skal også ivaretas ved tilgangsstyring. Dette gjelder f.eks. retten til å motsette seg *tilgang* til eller utlevering av helse- og personopplysninger jf. helsepersonelloven §§ 25 og 45, pasient- og brukerrettighetsloven § 5-3, forskrift om *tilgang* mellom virksomheter § 9 og pasientjournalloven § 17. Når *pasienten* har motsatt seg andres *tilgang* til *helseopplysninger* skal de opplysningene sperres for de som *pasienten* krever at ikke får *tilgang*.

3 TILGANGSSTYRING

Tilgangsstyringen skal etableres for å sikre at *virksomheten* fører kontroll med tilgang til *helse- og personopplysninger*. Valg av løsning skal baseres på en risikovurdering. I vurderingen kan avgjørende faktorer være *virksomhetens* størrelse, om tilgang gis til interne systemer eller om data for eksempel lagres i en skybasert løsning. *Virksomheten* må være forberedt på å håndtere eventuelle avvik og etablere systemer som forebygger slike.

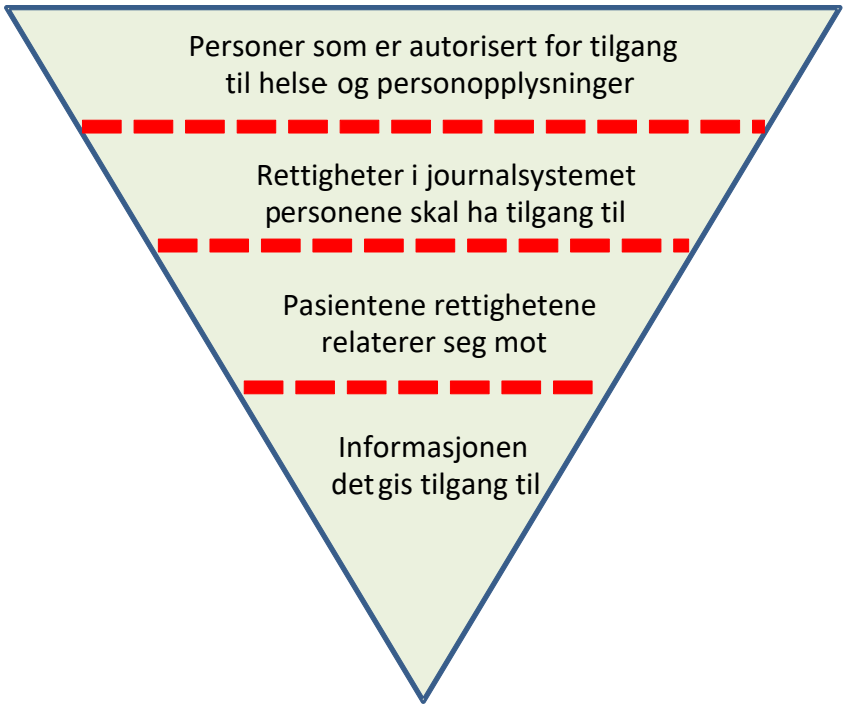
Autorisasjon for *tilgang* berører hvordan *virksomheten* foretar:

- *Autorisering* som er tildeling av rettigheter til å kunne lese, registrere, redigere og rette *helseopplysninger*
- *Autentisering* som sikrer identifisering av det *autoriserte* personellet
- Tilgjengeliggjøring av nødvendige og relevante *helseopplysninger* om bestemte *pasienter/brukere* for *autorisert* personell
- Kontrollerende tiltak

I tillegg kommer rettigheten *pasienten* har til å sperre egne *helseopplysninger* (se kap 3.3.1).

Dette kapitlet gir først en omtale av generelle krav for deretter å omtale *tilgang* ved ulike løsninger og situasjoner i *virksomheten*.

Figuren nedenfor illustrerer prinsippene for tilgangsstyring som en trakt hvor *tilgangen* skal være iht *tjenstlig behov* ved ytelse av helsehjelp til *pasienten*. *Tilgangen* skal regulere hvilke rettigheter (lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger) personen kan utføre for hvilke *pasienter*.



3.1 Personaladministrasjon i store virksomheter

Et særtrekk ved store *virksomheter* er egen funksjon for personaladministrasjon (HR) som ofte initierer *autoriseringen* av nye medarbeidere. Før den nyansatte begynner kan HR allerede ha registrert personalia i sentrale systemer og tildelt grunnleggende *tilganger* til nettverk og programmer. Samtidig har HR ordnet med ID-kort med nødvendige adganger og *tilganger* iht stillingskategori og rolle (se kap 3.3.2). ID-kortet kan være et Smartkort med sertifikat (se kap 3.4.4) som benyttes til flere funksjoner i *virksomheten*.

Ved slike tilfeller kan det kun være å tildele *autentisering* (se kap 3.4.4) for personellet som gjenstår. Dette ordnes vanligvis med personlig fremmøte med mottak av ID-kortet og første gangs kode for å få *tilgang* til nettverk og programmer. Personellet endrer deretter personlig kode for videre bruk.

Se også kapittel 3.3.4.2 Tilgangsstyring i små virksomheter.

3.2 Relevante og nødvendige helseopplysninger

Formålet med dokumentasjonsplikten som helsepersonellet har er bl.a. å sikre at opplysninger som er nødvendige og relevante for en forsvarlig behandling av *pasienten* blir nedtegnet og kan gjenfinnes.

Det er kun personell med *tjenstlig behov* som skal få *tilgang* til opplysningene, og de skal ikke få *tilgang* til flere opplysninger enn det som er relevant og nødvendig for å kunne gi helsehjelpen.

Det er reglene om *taushetsplikt* som regulerer hvilke og når *helseopplysninger* kan gjøres tilgjengelige. Hvilke *helseopplysninger* som kan gjøres tilgjengelige for personellet, vil være situasjonsavhengig knyttet til oppgavene vedkommende til enhver tid utfører.

Hva som er relevant og nødvendig vil imidlertid være de opplysningene som det i den aktuelle undersøkelses- og behandlingssituasjonen er behov for å ha tilgjengelig, for å kunne yte helsehjelp. Oftest må personellet selv vurdere hvilke *helseopplysninger* som er relevante og nødvendige for å gi helsehjelp. Dette kan være opplysninger som ikke er dekket i den tildelte *tilgangen*. For å løse dette kan selvautorisering benyttes for å gi nødvendig tilgang (se kap 3.3.5). Ved etablering av tilgangsstyringen må slike forhold vurderes slik at helsepersonell får den nødvendige *tilgang*.

3.3 Autorisasjon for tilgang

Med *autorisasjon* for *tilgang* menes at leder godkjenner at personell gis *tilgang* i journalsystemet og derigjennom *helseopplysninger* om *pasienter/brukere*.

Tilgangen skal gis med rettigheter til å lese, registrere (inklusive rekvirere, signere og kontrasignere), redigere og rette *helseopplysninger*. *Autorisasjon* for *tilgang* kan bare gis i den grad det er nødvendig for vedkommendes arbeid, er begrunnet ut fra *tjenstlig behov* og er i henhold til bestemmelser om *taushetsplikt*.

Databehandlingsansvarlig er ansvarlig for at *autorisasjon* for *tilgang* tildeles, administreres og kontrolleres og skal delegere myndighet for å tildele *autorisasjon* for *tilgang.*

I mindre og små *virksomheter* er det vanligvis den enkelte enhets ansvarlige leder som tildeler *autorisasjon* for *tilgang*. I dette ligger at ansvarlig leder, innen eget ansvarsområde, skal vurdere og godkjenne det enkelte personells behov for å få *tilgang* til *helseopplysninger*.

I store virksomheter vil *autoriseringen* oftest foregå som omtalt i kapittel 3.1.

Tildelt *autorisasjon* for *tilgang* skal sikre at den enkelte kan få *tilgang* til nødvendige *helseopplysninger* i samsvar med personellets ansvar og oppgaver, så langt lovbestemt *taushetsplikt* ikke er til hinder for det.

For personer som har ulike *roller* i *virksomheten*, skal autorisering skje for hver *rolle* uavhengig av vedkommendes øvrige roller.

3.3.1 Sperring

Dersom *pasienten* motsetter seg at andre får *tilgang* til *helseopplysninger*, skal opplysningene sperres. Sperringen skal kunne begrenses til de deler av journalen som *pasienten* bestemmer. Det skal fremgå av journalen om registrerte opplysninger er sperret.

Sperring skal kunne rettes mot bestemte personer eller grupper av personer i *virksomheten*. Kravet gjelder også personell hos eventuell *databehandler*.

Ønsker pasienten å gjøre unntak fra sperringen, skal dette være mulig. Det må da være mulig å registrere at *pasienten* har samtykket til at det gis *tilgang* til sperrede opplysninger og at kravet om sperring midlertidig er trukket tilbake.

Ved *tilgang* mellom *virksomheter* har *pasienten* rett til å reservere seg mot at helsepersonell i annen *virksomhet* gis *tilgang* til *helse- og personopplysninger*. *Autorisasjonen* for *tilgang* for helsepersonellet må ivareta dette kravet, slik at *pasientens* rettigheter ivaretas ved at *tilgang* til opplysningene sperres.

3.3.2 Rolle

Bruk av roller er en modell for tilgangsstyring som benyttes i noen virksomheter.

Med *rolle* menes en kategorisering av personell for å håndtere tilgangskontroll for å kunne yte, administrere og kvalitetssikre helsehjelpen til *pasienten/brukeren*. *Rolle* kan også knyttes til en organisatorisk enhet.

Rollebasert tilgangsstyring er relevant å benytte når samme bruker gjennom ulike funksjoner har ulike tilgangsbehov. *Tilgangen* styres da ved å tildele personen flere *roller* i *journalsystemet/EPJ* eller *fagsystemet*. Hver *rolle* skal tildeles selvstendig uavhengig av vedkommendes øvrige *roller* og ved behov gis ulike *autentiseringskriteria* (se kapittel 3.4.2).

Rettigheter til å lese, registrere, redigere og rette *helseopplysninger* i *rollene* fastsettes ut fra informasjonsbehovet ulike grupper ansatte vil ha ved ytelse av helsehjelpen. Rettighetene kan administreres i en *rollemal* (se kap 3.3.3) og ikke for den enkelte bruker.

Behov for *roller* og detaljstyring av *tilgang* for den enkelte *rolle* avhenger av *virksomhetens* størrelse og organisering (se kap 3.3.4.2 med eksempel for små virksomheter).

3.3.3 Rollemal

En *rollemal* beskriver hvilke *tilganger* de som opptrer i *rollen* skal ha og hvilke kategorier journalinformasjon de som innehar *rollen*, normalt skal gis *tilgang* til når det ytes helsehjelp.

3.3.4 Tilgang

Hvilken *autorisasjon* for *tilgang* som skal gis i en *virksomhet* skal være tilpasset risikoen ved *behandling* av *helseopplysninger*. Større *virksomheter* og *virksomheter* med særlig følsomme opplysninger vil gjerne ha flere og tydeligere funksjoner enn mindre *virksomheter*. *Autorisasjonene* for *tilgang* som gis må gi tilfredsstillende informasjonssikkerhet sammen med øvrige tiltak som *logging*, innsyn i *logg* og loggoppfølging.

Autorisasjon for *tilgang* skal tildeles i henhold til betryggende prosedyrer (se kapittel 4) og lovbestemt *taushetsplikt* skal vurderes og overholdes.

Teknisk personell med særskilt behov for *tilgang*, kan autoriseres for større mengder *helseopplysninger*. Eksempel er IKT-personell (se kapittel 3.3.4.8) som jobber med administrasjon av *journalsystem/EPJ* eller *fagsystem* eller databaseansvarlige som kan få *tilgang* til større mengder *helseopplysninger* i sitt daglige arbeide. Ved slik *tilgang* skal det iverksettes tiltak slik at mulig misbruk skal kunne forebygges. Eksempler på slike tiltak, i tillegg til *logging* som nevnt ovenfor, er:

- *Tilgang* gis via en personlig administratorkonto
- Engangspassord
- Sterk autentisering (sikkerhetsnivå 3 eller 4, se kapittel 3.4.4)
- Kryptering av lagrede opplysninger

3.3.4.1 Ytelse av helsehjelp

Ved ytelse av helsehjelp må personell gis mulighet til å søke opp og registrere relevante og nødvendige *helseopplysninger* i *pasientens* journal. Bare personell som er tildelt *autorisasjon* for *tilgang* kan få *tilgang* til *helseopplysninger*.

Eksempler på ytelse av helsehjelp til *pasient/bruker*:
- akuttbehandling av alvorlig syk pasient om natten
- poliklinisk besøk
- videokonsultasjon
- utarbeide henvisning
- helsehjelp hjemme
- fysioterapi

Tilgang til *helseopplysninger* i *pasientens* journal skal gis etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for å yte helsehjelp til *pasienten*. *Tilgang* skal styres slik at taushetspliktreglene ivaretas og at *tilgang* til *helseopplysninger* ikke gis til andre enn de som har *tjenstlig behov*. Dette gjelder også for *tilgang* i ordinære akuttsituasjoner, som ikke er å regne som selvautorisering (se kap 3.3.5).

I mindre og store *virksomheter* kan beslutningsstyrt *tilgang* være en måte å gjøre *helseopplysninger* tilgjengelig på. Ved bruk av beslutningsstyrt *tilgang* (se kap 3.3.4.3) skal personell første gang begrunne beslutningen i journalen.

Tildelingen av *autorisasjon* for *tilgang* skal føres inn i *autorisasjonsregisteret* (se kapittel 3.3.6).

3.3.4.2 Tilgangsstyring i små virksomheter

Med små *virksomheter* menes små legekontor, tannklinikker, psykologer, osv med få ansatte. Tilgangsstyringen kan forenkles, men prinsippet om *tilgang* ved *tjenstlig behov* må ivaretas. Tilgangsstyring kan bl.a. ivaretas med at:

- Alt personell benytter personlig brukernavn og passord. Fellesbrukere og utlån av passord benyttes ikke
- Selv om alt personell kan bli involvert i helsehjelpen, skal ikke alle ha normal *tilgang* til alle pasienters journaler. *Tilgangen* skal gis når det er nødvendig for å yte eller administrere helsehjelp. *Tilgang* kan bl.a. styres etter:
  - *Tilgang* til journaler for alle *pasienter* på en fastleges fastlegeliste
  - Avtalt time, f.eks. når *pasientens* fastlege ikke er til stede så kan vikar gis tilgang til journalen når *pasienten* har bestilt time
  - Rolle, for eksempel pasientansvarlig lege, helsesekretær, laboratoriepersonell

Pasienten har rett på sperring av sine helseopplysninger (sin journal), slik at for eksempel en ansatt ved *virksomheten*, som er nabo til pasienten, ikke skal få tilgang (se kap 3.3.1).

3.3.4.3 Beslutningsstyrt tilgang

Beslutningsstyrt *tilgang* (jf. EPJ Standard Del 2) kan benyttes for å gi *tilgang* til *helseopplysninger*.

Registrering av et besluttet tiltak begrunner behovet for opplysninger i journalen og åpner for at de som skal delta i gjennomføringen av tiltaket kan få *tilgang*.

Ved at personell skal delta i ytelsen av helsehjelp vil den registrerte beslutningen være grunnlag for å åpne journalen.

Tilgang i *journalsystem/EPJ* eller *fagsystem* kan styres automatisk ift ytelse av helsehjelpen ved at det gis et tidsvindu for når *tilgangen* er åpen. Det vil si at journalen/fagsystemet kan åpnes iht *autorisasjonen* for *tilgang*, for personell som er *autorisert* og yter eller kommer til å yte helsehjelp, før helsehjelpen gis og være tilgjengelig så lenge den ytes. Når ytelse av helsehjelpen avsluttes kan journalen stenges automatisk etter en angitt tid slik at journalen kan skrives ferdig og eventuell epikrise sendes. Eksempler er:

- journalen åpnes et fastsatt antall timer før en poliklinisk konsultasjon, inklusive videokonsultasjon, og lukkes etter et fastsatt antall timer
- journalen er åpen for inneliggende *pasienter*
- journalen åpnes ved mottak av henvisning og lukkes etter at helsehjelpen er gitt

Bruk av beslutningsstyrt *tilgang* er svært forskjellig i store og mindre virksomheter. I store virksomheter er ofte helsehjelpen planlagt (poliklinikk, pasientforløp, intern eller ekstern henvisning) og journalsystemet vil kunne hjelpe til med å gi *tilgang* til rett personell til rett tid.

3.3.4.4 Kortvarig tilgang

Kortvarig *tilgang* vil typisk gjelde for studenter, vikarer, konsulenter og ved kvalitetssikring av tjenesten.

Det skal opprettes avtale med personell slik at *virksomheten* har instruksjonsmyndighet og kan pålegge personellet instrukser og regler for bruk av systemene og *taushetsplikt*.

Personellet skal opprettes med *tilgang* i journalsystemet og med eget brukernavn og passord eller annen relevant *autentisering* (se kap 3.4.4) som samsvarer med behovet for *tilgang*.

For kortvarig *tilgang* anbefales det å registrere en sluttdato for *autorisasjonen* for *tilgang*.

3.3.4.5 Tilgang mellom virksomheter

Tilgang mellom *virksomheter* skal baseres på avtale mellom partene (se Veileder i personvern og informasjonssikkerhet ved *tilgang* til helseopplysninger mellom virksomheter på www.normen.no).

Ved slik *tilgang* skal personellets *autorisasjon* for *tilgang* til *helseopplysninger* i annen *virksomhet*:

- beskrive rettigheter og plikter som følger av *autorisasjonen* for *tilgang*
- være i samsvar med regler om *taushetsplikt*
- dokumenteres i *innhentende virksomhetens autorisasjonsregister*
- tidsbegrenses
- alltid vurderes og eventuelt endres når det oppstår endringer i ansvarsområder eller ansettelsesforhold

Tilgang til opplysninger i *utleverende virksomhet* kan kun gis dersom *pasienten* ikke har reservert seg. *EPJ-systemet* i *utleverende virksomhet* må ha funksjonalitet for å sperre *tilgang* slik at journalopplysninger gjøres utilgjengelige for enkeltpersoner, grupper av personell eller personell i andre *virksomheter* enn der journalnotatene er registrert (se kap 3.3.1).

Begge *virksomhetene* skal ha tekniske og organisatoriske løsninger som avgrenser *tilgangen* til *helseopplysninger* som minst ivaretar at:
- *helseopplysningene* ikke gjøres tilgjengelige dersom *pasienten/brukeren* har motsatt seg eller motsetter seg det
- det kun gis *tilgang* til *helseopplysninger* som er relevante og nødvendige for å yte, administrere eller kvalitetssikre helsehjelp til *pasienten/brukeren*
- personellet er *autorisert* for slik *tilgang*, og har *autentisert* seg ved bruk av *sikker autentiseringsløsning* (se kapittel 3.4.4).

Med relevante og nødvendige menes at personellet kun skal få *tilgang* til *helseopplysninger* som trengs for å kunne yte, administrere eller kvalitetssikre helsehjelpen. En hovedregel er at hvis ikke dette er mulig, skal det ikke åpnes for *tilgang* mellom *virksomheter*.

Autorisasjon for *tilgang* skal kun åpne for å lese *helseopplysninger* om *pasienten* ved *utleverende virksomhet*. Det vil si at *EPJ-systemet* i *utleverende virksomhet* må ha funksjonalitet for å begrense *tilgangen* til kun å lese *helseopplysninger* i systemet.

Innhentende og *utleverende virksomhet* skal til sammen ha tilgangsstyring som avgrenser *tilgangen* til *helseopplysninger* ved helsehjelp.

Innenfor rammen av hva som er avtalt mellom *virksomhetene*, skal ansvarlig leder i *innhentende virksomhet* beskrive rettigheter og plikter som følger av *autorisasjonen* for *tilgang* som gis personell for *tilgang* til *helseopplysninger* i *utleverende virksomhet*. Det enkelte personell skal informeres om rettighetene og pliktene.

Autorisasjon for *tilgang* skal tidsbegrenses ved at det angis starttidspunkt og sluttidspunkt. Sluttidspunktet må være reelt for de arbeidsoppgavene det enkelte personell skal utføre og knyttes til *tilgangene* vedkommende har.

Tildelt *autorisasjon* for *tilgang* skal dokumenteres i *autorisasjonsregisteret* i *innhentende virksomhet* (se kap 3.3.6).

3.3.4.6 Samarbeide om behandlingsrettede helseregistre

Etablering av samarbeid om *behandlingsrettet helseregistre* krever avtale mellom partene (se Samarbeid mellom *virksomheter* om felles journal, En veileder med avtaleeksempler på www.normen.no for avtalemaler).

Tildeling av *autorisasjon* for *tilgang* ved samarbeid om *behandlingsrettet helseregistre*, kan medføre behov for gjennomgang av tilgangsstyringen fordi det oppstår nye måter å yte helsehjelpen på. Likevel kan virksomhetene ta som utgangspunkt de samme reglene for autorisering som den enkelte *virksomhet* hadde før samarbeidet startet.

Tildelt autorisasjon for *tilgang* skal dokumenteres i *autorisasjonsregisteret* (se kap 3.3.6).

Ved et opphør av et *samarbeid* må *virksomhetene* ha prosedyrer som sikrer at personell blir fratatt sine *tilganger* iht avvikingen av samarbeidet.

3.3.4.7 Administrasjon av helsehjelp

Med administrasjon av helsehjelp menes for eksempel
- føring av timebok
- skrivestue som fører pasientjournalen
- skanning av dokumenter som overføres til *pasientens* journal
- behandling av refusjonskrav (behandlerkrav)
- beslutning om helsehjelp (vedtak i kommune)
- pasientkoordinering (for eksempel kontroll at helsehjelpen/tjenesten er levert til *pasienten/brukeren*)
- fordeling av hjemmebesøk

Personell som utfører disse oppgavene er ikke alltid helsepersonell, men skal likevel ha *tilgang* til *helseopplysninger* for å kunne utføre sitt arbeid.

Ved tildeling av *autorisasjon* for *tilgang* skal behovet for *tilgang* vurderes ift *tjenstlig behov*. Ved for eksempel føring av timebok vil administrativt personell ofte ha behov for *tilgang* til *pasientens* journal for å kunne planlegge helsehjelpen på en effektiv og riktig måte.

Prinsippene for beslutningsstyrt *tilgang* (se kap 3.3.4.3) kan også benyttes ved administrasjon. Pasientadministrasjonen skal uten hinder av *taushetsplikten* gis *pasientens* fødselsnummer og opplysninger om diagnose, eventuelle hjelpebehov, tjenestetilbud, innskrivnings- og utskrivningsdato samt relevante administrative data. Den enkelte skal likevel ikke gis *tilgang* til flere opplysninger enn det som er nødvendig for å ivareta det *tjenstlige behovet*.

Tildelt *autorisasjon* for *tilgang* skal føres inn i *autorisasjonsregisteret* (se kapittel 3.3.6).

3.3.4.8 IKT-personell

Med IKT-personell menes medarbeidere som jobber med drift av teknisk løsning eller forvaltning av elektronisk *pasientjournal/EPJ* eller *fagsystemer*.

Gjennom sitt arbeid kan IKT-personell ha behov for *tilgang* til større menger *helseopplysninger* og kan autoriseres for slik *tilgang*.

For eksempel kan IKT-personell ha ansvar som systemadministrator og få *tilgang* til større mengder *helseopplysninger*. Den enkelte medarbeider skal tildeles egen *autorisasjon* for *tilgang* og det er ikke anledning til å benytte fellesbruker.

Ved tildeling av *autorisasjon* for *tilgang* skal behovet for *tilgang* vurderes ift omfang og varighet.

Tildelt *autorisasjon* for *tilgang* skal føres inn i *autorisasjonsregisteret* (se kapittel 3.3.6).

3.3.4.9 Annen hjemmel for tilgang

Kvalitetssikring

Helseopplysninger kan gjøres tilgjengelig for kvalitetssikring og skal begrenses til de opplysninger som er nødvendige og relevante for formålet.

I *pasientens* journal skal det dokumenteres hvilke opplysninger som er gjort tilgjengelig for kvalitetssikring og hvem som har hatt *tilgang*. Det kan gjøres automatisk når vedkommende gis *tilgang*, samt at *autorisasjonsregisteret* vil gi informasjon om hva som har vært tilgjengelig.

Forskning

Prosjektleder i forskningsprosjektet skal sørge for at det etableres prosedyrer for tilgangsstyring til forskningsdata og forskningsfil slik at kun *autoriserte* for *tilgang* får forskningstilgang iht vedtatte prosedyrer i *virksomheten*. Vær klar over at den enkelte *virksomhet* kan ha sentrale føringer for slike prosedyrer.

Prosedyrene må ta hensyn til om forskningsfilen er direkte eller indirekte identifiserbar i det kravet til forholdsmessig sikring kan være ulikt.

Ved eventuell bruk av lyd- og bildeopptak må prosedyrene for tilgangsstyring omfatte dette.

Se også Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren på www.normen.no.

3.3.5 Selvautorisering

Selvautorisering (også kalt blålysfunksjon eller aktualisering) kan etableres som en mulighet for personell til å gi seg selv *tilgang* uten å følge vanlige regler for å få *tilgang* til *helseopplysninger*. Tilgang til funksjonen for selvautorisering skal tildeles personell som en egen rettighet. Det skal utarbeides egne prosedyrer for selvautorisering.

Eksempel på selvautorisering er at personell må yte helsehjelp i akuttsituasjoner og personell må ha *tilgang* ut over den tildelte *autorisasjonen*. Et annet eksempel er at helsepersonell må slå opp informasjon om *pasienten*, etter at ytelsen av helsehjelp er avsluttet, på bakgrunn av henvendelse fra *pasient* eller henvisende lege.

Begrunnelsen for selvautorisering skal dokumenteres ved hver bruk. Rent praktisk vil det si at personell må registrere en begrunnelse i *journalsystemet* for at journalen åpnes. Dette kan løses ved forhåndsdefinerte begrunnelser eller at personell selv registrerer begrunnelse.

Misbruk av selvautorisering som avdekkes ved kontroll, skal følges opp som om det var et *avvik*. For å fange opp missbruk skal et hvert *behandlingsrettet helseregister* loggføre og ha mulighet for å rapportere bruk av selvautorisering. Dette kan løses for eksempel med en intern e-post til ansvarlig for oppfølging av bruken eller ved uttak av og gjennomgang av rapporter over utført selvautorisering.

Hvis situasjonen til pasienten er så alvorlig at det kan begrunnes ut i fra liv og helse kan også selvautorisering brukes på informasjon som er underlagt reservasjon mot innsyn (se kap 3.3.1).

3.3.6 Autorisasjonsregister

Alle tildelte *autorisasjoner* for *tilgang* skal registreres i et *autorisasjonsregister* som minimum skal inneholde:

- informasjon om hvem som er tildelt *autorisasjon* for *tilgang*
- til hvilken rolle *autorisasjonen* for *tilgang* er tildelt
- formålet med *autorisasjonen* for *tilgang*
- tidspunkt for når *autorisasjonen* for *tilgang* ble gitt og eventuelt tilbakekalt
- informasjon om hvilken *virksomhet* den autoriserte er knyttet til
- personells *autorisasjon* for *tilgang* til *helseopplysninger* i annen *virksomhet* (kun om *tilgang* til *helseopplysninger* i annen *virksomhet* er tatt i bruk)

Det skal også registreres hvem (fysisk identifiserbar person) som har opprettet (registrert) *autorisasjonen* for *tilgang*.

Hver oppføring i *autorisasjonsregisteret* skal arkiveres i minimum 5 (jf. Normen kap 3.3.4) år fra det tidspunkt *autorisasjonen* for *tilgang* ble tatt ut av bruk. Oppføring i *autorisasjonsregisteret* gjelder i *virksomheten* og hos eventuell *databehandler*.

Autorisasjonsregisteret skal sikres mot uautorisert endring og sletting.

Autorisasjonsregister kan opprettes med for eksempel:
- Tekstdokument
- Regneark
- E-post som arkiveres
- Egen funksjon i *journalsystemet/EPJ* eller *fagsystem*

3.3.7 Fjerne og endre autorisasjon for tilgang

På samme måte som ved tildeling av *autorisasjon* for *tilgang* skal den enkelte enhets ansvarlige leder sørge for at *tilganger* oppdateres eller ugyldiggjøres. Lederen har ansvaret for jevnlig å følge opp og identifisere behov for fjerning og /endring.

Behov for endring er når en medarbeider:
- slutter og tildelt *autorisasjon* for *tilgang* skal deaktiveres fra en sluttdato
- begynner i ny stilling i samme *virksomhet*. Da må eksisterende *autorisasjon* for *tilgang* deaktiveres eller nye *tilganger* tilføres ved å fjerne eller føye til nye funksjoner
- skal har permisjon og *autorisasjon* for *tilgang* deaktiveres frem til permisjonen er over

Ved fjerning av *autorisasjon* for *tilgang* skal *autorisasjonsregisteret* (se kapittel 3.3.6) oppdateres med dato og klokkeslett for når *autorisasjonen* for *tilgang* ble trukket tilbake.

3.4 Autentisering

Med autentisering menes prosessen som gjennomføres ved pålogging til *journalsystem/EPJ* eller *fagsystem* for å bekrefte at personellet er den vedkommende utgir seg for å være.

Som eksempel fra hverdagen, med bruk av nettbank, benytter de fleste 11-sifret fødselsnummer for å gi en påstått identitet. For å bekrefte identiteten krever nettbanken at det registreres en 6-sifret kode fra kodebrikke og et passord. Stemmer disse, gis det tilgang til nettbanken.

Formålet med *autentiseringen* er å sikre at det er rett person som gis *tilgang* til *helseopplysninger*. For å sikre identifisering over tid må personen identifiseres med en varig identitet som for eksempel 11-sifret fødselsnummer, HPR-nummer, HER-id, eller tilsvarende.

Autentiseringen knyttes også til styrken på autentiseringskriteriene (se kapittel 3.4.4) som for eksempel:
- brukernavn og passord
- brukernavn og passord kombinert med kode som mottas som SMS
- bruk av elektronisk identitetsbevis (for eksempel BankID, Buypass eller Commfides)

Styrken på *autentiseringen* skal tilpasses behovet for å være sikker på at personellet er den rette personen, og skal være i henhold til gjennomført risikovurdering.

Flere personer skal ikke benytte samme *autentisering* som vil si at det enkelte personell skal ha unik *autentisering*. Fellesbruker og felles passord er ikke tillatt.

3.4.1 Tildeling av autentiseringskriterier

Tildeling av autentiseringskriterier (som brukernavn og passord) skal gjennomføres på en betryggende måte.

Tildelingen bør innbefatte personlig oppmøte og identifisering vha. legitimasjon med mindre den som registrerer brukeridentiteten kjenner personellet fra før.

3.4.2 Flere roller

En spesiell utfordring er at en og samme person kan ha flere *roller* og *autentiseringen* må sikre identifisering av personen i korrekt *rolle* i hvert enkelt tilfelle. Det er ikke et krav om unik *autentisering* i hver *rolle*, men det kan ved behov stilles krav om dette. Fastsettelse av behovet skal være i henhold til gjennomført risikovurdering.

3.4.3 Flere ansettelsesforhold

Er personellet representert med flere ansettelsesforhold i *virksomheten* skal hvert ansettelsesforhold identifiseres ved *autentiseringen*. Som eksempel at personellet er ansatt i virksomheten tre dager i uken og innleid personell øvrige dager i uken.

Ved slike tilfeller kan personellet logge seg på systemet og velge *virksomhet* og eventuell *rolle* innenfor den *virksomheten* som er valgt.

3.4.4 Styrken på autentiseringen

Autentiseringen kan ha ulik styrke og eksemplene nedenfor er hentet fra dokumentet ”Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor[2]”.

Styrken på *autentiseringen* i rammeverket omtales som sikkerhetsnivå 1 til 4.

Eksempler på tekniske løsninger som vil tilfredsstille de forskjellige sikkerhetsnivåene er:

Sikkerhets-nivå	Løsning
1	Ukjent bruker med selvvalgt passord og selvvalgt brukernavn
2	Identifisert bruker med tildelt brukernavn og førstegangs passord, tvungen bytte av passord
3	Tildelt brukernavn og engangspassord tilsendt på mobiltelefon (som SMS) eller personlig sertifikat
4	Løsninger basert på Public Key Infrastructure (PKI). Iht til gjeldende regelverk må løsningene være selvdeklarert i Nasjonal kommunikasjonsmyndighet i forhold til om de oppfyller krav i Kravspesifikasjon for PKI i offentlig sektor[3] når det gjelder Person Høyt og Virksomhet (*personlig kvalifisert sertifikat*). Eksempler er BankID, BankID på mobil, Buypass eller Commfides

Se også Faktaark 31 - Passord og passordhåndtering og Faktaark 38 - Sikkerhetskrav for systemer på www.normen.no.

[2] https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/
[3] https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/

Nedenfor angis hvilken *autentisering* som bør benyttes.

3.4.5 Internt i virksomheten

Risikovurdering skal ligge til grunn for valg av tilstrekkelig sikkerhetsnivå (se kap 3.4.4) ved pålogging til interne systemer (nettverk, EPJ internt o.l.). Risikovurdering bør omfatte momenter som:

- *Virksomhetens* størrelse, antall brukere og antall funksjoner
- Antall lokasjoner
- Antall og type systemer og tjenester, herunder volum på sensitive personopplysninger, som *autentiseringen* gir *tilgang* til

Større *virksomheter* med et stort antall arbeidsstasjoner (klienter) og personell, har i utgangspunktet et risikopotensiale som tilsier behov for sikkerhetsnivå 3 (se kap 3.3.4) for å oppnå tilstrekkelig sikkerhet.

For mindre virksomheter skal minimum sikkerhetsnivå 2 benyttes (se kap 3.3.4) med tildelt brukernavn og passord med en fastsatt kompleksitet (for eksempel kan systemet settes opp til å kreve passord med minimum 7 tegn, minst ett tall og både store og små bokstaver).

Ved bruk av mobilt utstyr, hjemmekontor og trådløs kommunikasjon skal *autentiseringen* ikke innebære økt risiko utover det som gjelder for stasjonært utstyr. En risikovurdering må vise at autentiseringsløsningen gir tilstrekkelig sikkerhet.

3.4.6 Portalløsning og skyløsning

Autentisering for bruk av kun administrative funksjoner uten *helseopplysninger* (som for eksempel bestilling og avbestilling av time uten at grunnen for timebestilling oppgis) skal gjøres med minimum sikkerhetsnivå 3 (se sikkerhetsnivå 3 i kapittel 3.4.4).

Autentisering for *tilgang* til og kommunikasjon av *helseopplysninger* i løsninger levert av helsepersonell (inklusive timebestilling der *pasient/bruker* oppgir grunnen for bestilling av time og reseptfornying) skal gjøres med *personlig kvalifisert sertifikat* eller annen sikker autentiseringsløsning. Ved bruk av annen autentiseringsløsning må en risikovurdering vise at denne har tilstrekkelig sikkerhet (se sikkerhetsnivå 4 i kapittel 3.4.4).

Se Personvern og informasjonssikkerhet i kontakten med pasient/bruker, En veileder i bruk av portalløsninger, SMS og e-post og Veileder i bruk av skytjenester til behandling av helse- og personopplysninger, Ansvar, avtaler og informasjonssikkerhet på www.normen.no.

3.4.7 Tilgang mellom virksomheter

Personell i *innhentende virksomhet* skal *autentiseres* ved bruk av *sikker autentiseringsløsning* slik at det er sikkerhet for at personen som gis *tilgang* i *EPJ-systemet* i *utleverende virksomhet* faktisk er den vedkommende utgir seg for å være.

Eksempel på *sikker autentiseringsløsning* er bruk av *personlig kvalifisert sertifikat* (se sikkerhetsnivå 4 i kapittel 3.4.4).

Andre løsninger som kan vurderes er personlig sertifikat (se sikkerhetsnivå 3 i kapittel 3.4.4) eller engangspassord på mobiltelefon (se sikkerhetsnivå 3 i kapittel 3.4.4). Velges en løsning som ikke er basert på *personlig kvalifisert sertifikat* må begge *virksomhetene* gjennomføre en risikovurdering som viser at autentiseringsløsningen har tilstrekkelig sikkerhet.

3.4.8 Samarbeid om behandlingsrettede helseregistre

Autentiseringen følger de samme kravene som internt i *virksomheten* (se 3.4.5) under forutsetningen at kommunikasjonen mellom *virksomhetenes* nettverksoner hvor *helseopplysninger* behandles, er kryptert iht "Kravspesifikasjon for PKI i offentlig sektor"[4].

3.5 Kontroll av tilganger

3.5.1 Tildelte autorisasjoner for tilgang

Gjennomgang og kontroll av tilgangsstyringen, herunder tildelte *autorisasjoner* for *tilgang*, må organiseres og bør foretas av den enkelte leder:

- Minimum årlig (gjerne i forbindelse med sikkerhetsrevisjon)
- Ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde
- Ved sikkerhetsbrudd for det informasjonsområdet som ble berørt av bruddet

Virksomhetens ledelse skal påse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk *tilgang* til *helseopplysninger* i et *behandlingsrettet helseregister* (inkl *elektronisk pasientjournal (EPJ)*) eller i et *fagsystem*.

Dersom kontrollen fører til mistanke om at det har skjedd en urettmessig *tilgang*, skal *virksomhetens* ledelse varsles. Forøvrig skal hendelsen behandles iht. etablerte prosedyrer for avviksbehandling, særlig med henblikk på å få avklart om eksisterende tilgangskontroll er god nok.

Dersom kontrollen viser at det har skjedd en urettmessig *tilgang*, skal Datatilsynet informeres. Videre skal *virksomhetens* ledelse vurdere om *pasienten/brukeren* skal informeres.

3.5.2 Logger

Logger skal benyttes som en del av kontrollen av tilgangsstyringen og skal analyseres for å oppdage brudd.

Se Faktaark 15 - Hendelsesregistrering og oppfølgning på www.normen.no for bruk av *logger* til kontroll.

[4] https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/

4 EKSEMPLER PÅ PROSEDYRER

4.1 Tildeling av autorisasjon for tilgang

Hensikt/omfang

Sikre at personell tildeles autorisasjonen for tilgang til helseopplysninger iht tjenstlig behov og taushetsplikten.

Ansvar/målgruppe

Ansvarlig leder skal tildele autorisasjon for tilgang til den enkelte medarbeider.

Gjennomføring

1. Taushetserklæring leses og underskrives av den ansatte
2. Sikkerhetsinstruks leses og underskrives av den ansatte
3. Leder skal deretter informere <IT-avdelingen> om behov for brukertilganger. Vær spesielt oppmerksom på hvor lenge det er behov for tilgangen samt nivå på tilgang. Benytt <felles> autorisasjonsskjema for de ulike systemer. Disse finnes på <Virksomhet>s Intranettsider
4. Leder er ansvarlig for å oppbevare en kopi av underskrevet erklæring og instruks samt autorisasjonsskjema for alle som inngår i personalansvaret. Original autorisasjonsskjema sendes i tillegg til <IT-avdelingen>
5. <IT-avdelingen> er ansvarlig for å føre den tildelte autorisasjonen for tilgang inn i autorisasjonsregisteret

Ved endringer av ansvar eller organisasjonsmessig tilhørighet internt i <Virksomhet> skal brukerens tilganger i informasjonssystemet vurderes. <IT avdelingen> skal informeres om eventuelle relevante endringer i behov for tilgang på informasjonssystemene. Leder skal oppbevare kopi av alle meldte endringer.

4.2 Kontroll av tildelte autorisasjoner for tilgang

Hensikt/omfang

Sikre at personell er tildelt autorisasjonen for tilgang til helseopplysninger iht tjenstlig behov og taushetsplikten.

Ansvar/målgruppe

Ansvarlig leder skal minimum årlig kontrollere tildelte autorisasjoner for tilgang for egne medarbeidere.

Gjennomføring

1. <IT-avdelingen> vil regelmessig og minimum årlig sende ut oversikt over brukere og brukertilganger til leder med personalansvar
2. Leder skal så snart som praktisk mulig etter mottak, verifisere at oversikten er korrekt og at tilgangene er berettigede, dvs reflekterer ansvar og organisasjonsmessig tilhørighet
3. Tilbakemelding skal uansett sendes og eventuelle endringer, feil og mangler skal sendes <IT-avdelingen> på e-post
4. Leder skal oppbevare kopi av alle meldte endringer

4.3 Selvautorisering - logging og oppfølging av logger

Hensikt/omfang

Sikre at bruk av selvautorisering logges og følges opp.

Ansvar/målgruppe

Ansvarlig leder skal følge opp bruk av selvautorisering.

Gjennomføring

1. <IT-avdelingen> skal sørge for at det logges all bruk av selvautorisering
2. <IT-avdelingen> sender logg som viser bruk av selvautorisering til ansvarlig leder som skal følge opp bruken
3. Leder skal gå gjennom den enkelte bruk og kontrollere at bruken er iht ytelse av helsehjelp til pasienten/brukeren og at begrunnelsen er tilstrekkelig
4. Er bruken av selvautorisering uklar eller ikke tilstrekkelig begrunnet skal personellet kontaktes og leder innhente forklaring og underlag på bruken
5. Basert på registrert eller innhentet forklaring og underlag treffer leder beslutning om det er grunnlag for personalmessige konsekvenser
6. Personalmessige konsekvenser avtales nærmere med <personalavdelingen> og personellet informeres skriftlig om beslutningen
7. Den skriftlige beslutningen arkiveres i personellets personalmappe

5 VEDLEGG

5.1 Anbefalte dokumenter ifm. informasjonssikkerhet

Dokumentene i tabellen nedenfor er relevante i forbindelse med tilgangsstyring*:*

Dokument	Relevans
Faktaark 15 – Hendelsesregistrering og oppfølging	Faktaarket omtaler bl.a. bruk av *logger* til kontroll.
Faktaark 31 – Passord og passordhåndtering	Faktaarket gir innspill til styrke på passord, frekvens for bytte av passord, med mer
Faktaark 38 – Sikkerhetskrav for systemer	*Normens* krav til systemer (*EPJ* og *fagsystemer*). Dette faktaarket beskiver alle krav *leverandøren* av *EPJ-system* / *fagsystem* skal ivareta i systemet
Faktaark 47 – Autorisasjonsregister	Faktaarket omtaler innhold i *autorisasjonsregisteret* og hvordan det kan etableres

5.2 Definisjoner

Definisjoner er hentet fra *Normen*. Nye begrep er definert og samlet etter definisjoner fra *Normen*. Definerte ord er markert i *kursiv* i teksten.

Definisjoner fra *Normen* (4. juni 2015)

-A-

Med ”***administratorrettighet***” menes i *Normen* øverste tilgangsnivå til system, server, database, og sikkerhetsbarriere. Tilgangsnivået har som oftest rettigheter til å utføre alle operasjoner.

Med ”***autentisere***/***autentisering***” menes i *Normen* prosessen som gjennomføres for å bekrefte en påstått identitet.

Med ”***autorisere/autorisert/autorisasjon***” menes i *Normen* at en person i en bestemt rolle kan gis eller er gitt bestemte rettigheter til lesing, registrering, redigering, retting, sletting og/eller sperring av *helse- og personopplysninger. Autorisasjon* kan bare gis i den grad det er nødvendig for vedkommendes arbeid, er begrunnet ut fra *tjenstlig behov* og er i henhold til bestemmelser om *taushetsplikt*.

Med ”***autorisasjonsregister***” menes i *Normen* et *register* over utstedte *autorisasjoner* som føres av den *databehandlingsansvarlige.*

Med "***avvik***" menes i *Normen* enhver håndtering av *helse- og personopplysninger* som ikke utføres i henhold til gjeldende regelverk, retningslinjer og/eller prosedyrer, samt andre sikkerhetsbrudd.

-B-

Med "***behandling***" menes i *Normen* enhver formålsbestemt bruk av *helse- og personopplysninger*, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter, jf. helseregisterloven § 2 c), pasientjournalloven § 2 b) og personopplysningsloven § 2 nr. 2).

Med "***behandlingsrettet helseregister***" menes i *Normen* pasientjournal og informasjonssystem eller annet register, fortegnelse eller lignende, der *helseopplysninger* er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen og som skal gi grunnlag for helsehjelp eller administrasjon av helsehjelp til enkeltpersoner, jf. pasientjournalloven § 2 d). Se også *elektronisk pasientjournal (EPJ)* og *tjenestedokumentasjon*.

Med "***bruker***" menes i *Normen* en person som anmoder om eller mottar tjenester omfattet av helse- og omsorgstjenesteloven som ikke er helsehjelp, jf. pasient- og brukerrettighetsloven § 1-3 bokstav f.

-D-

Med "***databehandler***" menes den som *behandler helse- og personopplysninger* på vegne av den *databehandlingsansvarlige*, jf. personopplysningsloven § 2 nr. 5). Det presiseres at en *databehandler* er en ekstern person eller *virksomhet* utenfor den *databehandlingsansvarliges virksomhet*. Det vil si at den *databehandlingsansvarliges* egne medarbeidere ikke er dennes *databehandlere*.

Med "***databehandlingsansvarlig***" menes den som bestemmer formålet med *behandlingen* og hvilke hjelpemidler som skal brukes, hvis ikke *databehandlingsansvaret* er særskilt angitt i loven eller i forskrift i medhold av loven, jf. helseregisterloven § 2 e), pasientjournalloven § 2 e) og personopplysningsloven § 2 nr. 4) (her benyttes begrepet "behandlingsansvarlig"). Det presiseres at det er *virksomheten* som er *databehandlingsansvarlig* for *behandling* av *helse- og personopplysninger*. Ansvaret skal ivaretas av den daglige ledelsen av *virksomheten*, og *virksomheten* er pliktsubjekt.

-E-

Med "***elektronisk pasientjournal (EPJ)***" menes i *Normen* elektronisk ført samling eller sammenstilling av nedtegnede/registrerte opplysninger om en *pasient* i forbindelse med helsehjelp, se også helsepersonelloven § 40 første ledd og forskrift om pasientjournal § 3 a). Dette inkluderer både somatisk og psykiatrisk journal o.a., hver for seg eller samlet. Se også *behandlingsrettet helseregister*.

Med "***elektronisk pasientjournalsystem (EPJ-system)***" menes i *Normen* elektroniske systemer med nødvendig funksjonalitet for å registrere, søke frem, presentere, kommunisere,

redigere, rette og slette opplysninger i *elektronisk pasientjournal (EPJ).* Dette inkluderer både radiologisystemer, systemer for somatisk og psykiatrisk journal, pasientadministrative systemer og andre systemer som inneholder *helseopplysninger.*

-F-

Med "***fagsystem***" menes i *Normen* en applikasjon eller et IT-system som *behandler helse- og personopplysninger*. Begrepet systemløsning brukes også om et *fagsystem*. Eksempler på *fagsystem* er: pleie- og omsorgssystem (PLO), legekontorsystem og barnevernsystem. Opplysninger i ulike *fagsystemer* kan både utgjøre *elektronisk pasientjournal (EPJ)* og annen *tjenestedokumentasjon*.

-H-

*"**helse- og personopplysninger**"* benyttes i *Normen* som en fellesbetegnelse for *helseopplysninger* og/eller *personopplysninger* innenfor *Normens* virkeområde.

*Med "***helseopplysninger***" menes i* Normen *taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson, jf. helseregisterloven § 2 a) og pasientjournalloven § 2 a).*

Med "***helseregister***" menes i *Normen* registre, fortegnelser, m.v. der *helseopplysninger* er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen, jf. helseregisterloven § 2 d).

-L-

Med "***logg***" menes i *Normen* et logisk *register* der hendelser og aktiviteter i informasjonssystemet er nedtegnet, se neste definisjon. Slik logg kan også benevnes "***sikkerhetslogg***"

-P-

Med "***pasient***" menes i *Normen* en person som henvender seg til helse- og omsorgstjenesten med anmodning om helsehjelp, eller som helse- og omsorgstjenesten gir eller tilbyr helsehjelp i det enkelte tilfelle, jf. pasient- og brukerrettighetsloven § 1-3 bokstav a.

"***pasientopplysninger***", se *helse- og personopplysninger.*

Med "***personopplysninger***" menes i *Normen* opplysninger og vurderinger som kan knyttes til en enkeltperson, jf. personopplysningsloven § 2 nr. 1).

-R-

Med "***register***" menes i *Normen* en logisk sammenstilling av opplysninger. En database eller et regneark er en teknisk løsning for et *register*.

Med ”***registrert/den registrerte***” menes i *Normen* den som opplysninger kan knyttes til, jf. personopplysningsloven § 2 nr. 6. Eksempler og begreper som brukes om *den registrerte* er søker, *pasient/bruker* og tjenestemottaker. En ansatt kan være omfattet av begrepet.

-T-

Med ”***taushetsplikt***” menes i *Normen* lovpålagt eller avtalt plikt til å hindre at andre får adgang eller kjennskap til *helse- og personopplysninger*, jf. helsepersonelloven § 21, helseregisterloven § 17, pasientjournalloven § 15, helse- og omsorgstjenesteloven § 12-1, spesialisthelsetjenesteloven § 6-1 og forvaltningsloven §§ 13 til 13e, samt annen informasjon med betydning for informasjonssikkerheten, jf. personopplysningsforskriften § 2-9. *Taushetsplikt* innbefatter både en passiv plikt til å tie og en plikt til aktivt å hindre uvedkommende i å få kunnskap om taushetsbelagte opplysninger.

Med ”***tilgang***” menes i *Normen* at *helse- og personopplysninger* om en eller flere bestemte *pasienter/brukere* er eller gjøres tilgjengelige for *autorisert* personell. Beslutning om *tilgang* til *behandlingsrettede helseregistre* skal treffes etter en konkret vurdering basert på at det ytes helsehjelp til *pasienten. Tilgang* til *fagsystemer* i forbindelse med ytelser til *pasient/bruker* skal iverksettes basert på *tjenstlig behov*. *Tilgang* i forbindelse med kvalitetssikring og administrative oppgaver skal også besluttes ut fra *tjenstlig behov*.

Med ”***tjenstlig behov***” menes i *Normen* at personer med nærmere bestemte arbeidsoppgaver, trenger nødvendige *helse- og personopplysninger* for å yte helsehjelp, omsorgstjeneste og/eller utføre administrasjon i forbindelse med dette. Dersom *pasienten* har sperret hele eller deler av *helse- og personopplysningene* kreves særskilt hjemmel for *tilgang* til disse.

-V-

Med ”***virksomhet***” menes i *Normen* juridisk enhet som helseforetak, *kommune*, sykehus, legepraksis, tannklinikk, apotek, apotekkjede, røntgeninstitutt, frittstående laboratorium, universitet, høyskole, stiftelse m.v.

Nye definisjoner i denne veilederen:

Med ***”rolle”*** menes i dette dokumentet en funksjon i en virksomhet som utøves av en tjenesteyter (person).

Med ***”rollemal”*** menes i dette dokumentet et sett av *tilganger* som gis til alle tjenesteytere som innehar en rolle.

Til definisjonen av **”*tilgang*”** ovenfor er følgende tillegg relevant:
I merknadene til pasientjournalloven § 19 omfatter uttrykket "tilgjengelige" både tilgang til helseopplysninger, ved at personell gis adgang til å søke opp de aktuelle helseopplysningene i systemet, og at opplysningene gjøres tilgjengelige ved at de utleveres.
Videre er tilgang definert i forskriften om tilgang til helseopplysninger mellom virksomheter slik: ”Med tilgang menes at helsepersonell gis adgang til direkte elektronisk å hente frem helseopplysninger om pasienter.”

5.3 Referanser

Nedenfor vises referanse til regulatoriske bestemmelser og dokumenter som er relevante for denne veilederen:

- Faktaark 15 – Hendelsesregistrering og oppfølging
- Forskrift om pasientjournal
- Helseforskningsloven
- Helsepersonelloven
- Helseregisterloven
- Norm for informasjonssikkerhet
- Pasientjournalloven
- Pasient- og brukerrettighetsloven
- Personopplysningsloven
- Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor, april 2008

5.4 Deltagere i referansegruppen

Følgende har deltatt i referansegruppen:

Navn	Organisasjon	Stilling/rolle	e-post
Hanne Kolflaath	Acos	Forretningsansvarlig Levekår	hanne@acos.no
Stian Grønhaug	Acos		stian@acos.no
John Kraabøl	CGM		john.kraaboel@cgm.com
Camilla Nervik	Datatilsynet	Seniorrådgiver	camilla.nervik@datatilsynet.no
Grete Alhaug	Datatilsynet	Seniorrådgiver	Grete.Alhaug@Datatilsynet.no
Jon Berge Holden	Difi		JonBerge.Holden@difi.no
Trond Elde	DIPS	Produktansvarlig IAM	tre@dips.no
Aasta Hetland	Direktoratet for e-helse	Sekretariatet for Normen	Aasta.Hetland@ehelse.no
Hólmar Õrn Finnsson	Direktoratet for e-helse		Holmar.Orn.Finnsson@helsedir.no
Ida Martinussen	Direktoratet for e-helse		Ida.Martinussen@ehelse.no
Jan Henriksen	Direktoratet for e-helse	Sekretariatet for Normen	jan@infosec.no
Knut Henrik Andersen	Direktoratet for e-helse	Sekretariatet for Normen	knut@incertus.no
Odd-Roar Wangen	Direktoratet for e-helse		Odd-Roar.Wangen@ehelse.no
Hallgeir Nisja	Helse Midt Norge	Rådgiver sikkerhet Administrasjon	Hallgeir.Nisja@hemit.no
André Breivik	Helse Vest IKT	Konsulent Samhandling	andre.nordvik.breivik@helse-vest-ikt.no
Heidi Thorstensen	HSØ	Informasjonssikkerhetsleder	uxthei@ous-hf.no
Johan Krüger	HSØ	Informasjonssikkerhetsleder	johan.kruger@sshf.no
Petter Hurlen	Legeforeningen		Petter@hurlen.no
Irene Oksdøl	Oslo kommune Helseetaten Fagsystemavdelingen	Spesialkonsulent	irene.oksdol@hel.oslo.kommune.no
Rune Gomo	Visma	Produkteier SamPro	Rune.Gomo@visma.no