NORMEN

# Veileder for tilgang til helse- og person-opplysninger

Versjon 2.0

17. mars 2022

Utarbeidet med støtte fra Direktoratet for e-helse

Vedtatt av styringsgruppen for Normen

Denne veilederen er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Normen forvaltes av Styringsgruppen for Normen, etter Normens forvaltningsmodell.

Normen skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt. Innbyggere og ansatte skal være trygge på at opplysninger om dem behandles på en sikker måte i helse- og omsorgssektoren. Normen skal bidra til at virksomheter i helse- og omsorgssektoren kan ha gjensidig tillit til hverandre, ved å etablere mekanismer og regler som sørger for at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Alt om Normen, Normens krav og veiledningsmateriell finnes på www.normen.no.

En til enhver tid oppdatert versjon av veilederen finnes på www.normen.no. Dersom du har spørsmål knyttet til veilederen kan du sende spørsmål og kommentarer til: sikkerhetsnormen@ehelse.no

# Innhold

# 1. Innledning

## 1.1 Bakgrunn

Virksomheter og helsepersonell som yter helsehjelp er ansvarlige for å gi forsvarlig helsehjelp. Virksomheter og helsepersonell må også sikre at behandling av helse- og personopplysninger som utføres i den forbindelse skjer på en måte som ivaretar taushetsplikten og sikrer pasientenes personvern. Ved ytelse av helsehjelp vil det ofte være relevant for helsepersonell å ha tilgang til opplysninger i pasientens journal. Virksomheter som yter helsehjelp, er ansvarlig for å sørge for at relevante og nødvendige helseopplysninger om pasienten er tilgjengelig for helsepersonell og annet samarbeidende personell når de trenger det for å yte helsehjelp til pasienten.

Det er reglene om taushetsplikt i helsepersonelloven som regulerer hvilke opplysninger som kan gjøres tilgjengelig og når opplysningene skal gjøres tilgjengelig. Virksomheten må tilgjengeliggjøre opplysningene på en måte som ivaretar kravene til informasjonssikkerhet.

Tilgangsstyring er ett av flere virkemidler for å ivareta kravene til informasjonssikkerhet. Tilgangsstyringen skal gi personell tilgang til nødvendige helseopplysninger ut fra tjenstlig behov og samtidig hindre uautorisert bruk og uberettiget innsyn i opplysninger.

## 1.2 Tema for veilederen

Denne veilederen skal gi veiledning til og bidra til etterlevelse av kravene Normen stiller til etablering av tilfredsstillende tilgangsstyring innad i virksomheten.

Veilederen gjelder tilgangsstyring i behandlingsrettede helseregistre for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte pasient. Veilederen omtaler hovedsakelig temaene autorisering, autentisering og kontroll av tilgang til helse- og personopplysninger, men gir også en overordnet innføring i generelle prinsipper for tilgangsstyring.

Veilederen er tiltenkt å gi målgruppene hjelp til blant annet å

- få oversikt over generelle prinsipper for tilgangsstyring
- forstå prinsipper for autorisering, autentisering og kontroll av tilganger
- få en forståelse for tilgangsstyring i virksomheter og på tvers av virksomheter i helse- og omsorgssektoren
- beslutte tilstrekkelige tiltak for tilgangsstyring ved behandlingen av helse- og personopplysninger.

Veilederen bør ses i sammenheng med Normens vedlegg «Oversikt over Normens krav»[1] som blant annet utdyper tekniske sikkerhetskrav for systemer som er relevant for å blant annet få på plass en helhetlig tilgangsstyring.

Veiledning om tilgang mellom virksomheter skal innarbeides i løpet av 2022.

[1] Normen 6.0 – Oversikt over Normens krav

## 1.3 Målgruppe

Målgruppen for veilederen er virksomheter som omfattes av Normen og som skal sikre etterlevelse av Normens krav til tilgangsstyring. Veilederen vil være særlig relevant for systemforvalter og personell som jobber praktisk med tilgangsstyring i virksomheten, men også andre roller som for eksempel dataansvarlig, informasjonssikkerhetsleder og sikkerhetsleder.

Veilederen kan også være nyttig for samarbeidspartnere til helse- og omsorgssektoren, som på grunn av sin leveranse er omfattet av Normen 6.0 gjennom avtale med virksomheten eller Norsk Helsenett SF. Eksempler på slike samarbeidspartnere er databehandlere og systemleverandører av elektronisk pasientjournal (EPJ) og fagsystemer.

## 1.4 Krav i Normen

Kapittel 5.2 i Normen 6.0 omtaler tilgangsstyring og er delt opp i tre hovedtemaer:

- 5.2.1. Autorisering
- 5.2.2. Autentisering
- 5.2.3. Kontroll av tilgang.

Ovennevnte hovedtemaer vil være de mest sentrale temaene i denne veilederen. Det er imidlertid også andre krav i Normen 6.0 til virksomhetens arbeid med tilgangsstyring, herunder følgende temaer:

- 3. Risikostyring (med tilknyttede underkapitler)
- 4.2.5 Tilgjengeliggjøring og utlevering av opplysninger i behandlingsrettet helseregister
- 5.1.2. Opplæring og kompetanse
- 5.1.3. Opphør av arbeidsforhold.

## 1.5 Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk

### 1.5.1 Generelle krav til håndtering av helse- og personopplysninger

I pasientjournalloven § 22 er det krav om at dataansvarlig og databehandler må gjennomføre tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå med hensyn til risikoen for de registrertes rettigheter og friheter. For å oppnå et egnet sikkerhetsnivå fastsetter bestemmelsen at den dataansvarlige og databehandleren blant annet må sørge for tilgangsstyring, logging og etterfølgende kontroll på områdene som loven regulerer. I tillegg er det i pasientjournalloven § 23 fastsatt at dataansvarlig må etablere tekniske og organisatoriske tiltak for å sikre og påvise sin egen etterlevelse av personvernforordningen. Videre fremgår det av bestemmelsen at tiltakene skal dokumenteres.

Pasientjournalloven §§ 22 og 23 bygger på, og henviser til, personvernforordningen artikkel 24 og 32. I motsetning til pasientjournalloven stilles det ikke i personvernforordningen et

eksplisitt krav om tilgangsstyring. Tilgangsstyring benyttes imidlertid ofte som et tiltak for å ivareta personopplysningenes konfidensialitet og tilgjengelighet. Velfungerende tilgangsstyring vil blant annet redusere risikoen for ulovlig og uautorisert behandling av personopplysningene.

## 1.5.2 Krav til tilgjengelighet

Med «tilgjengelighet» menes i Normen at helse- og personopplysninger som skal behandles, er tilgjengelig til den tid og på det sted det er behov for opplysningene.[2] Kravet til tilgjengelighet kommer til uttrykk i særlovgivningen for helse- og omsorgssektoren, som har bestemmelser om når pasienters helse- og personopplysninger skal gjøres tilgjengelig for helsepersonell og andre. For behandlingsrettet helseregister er det fastsatt i pasientjournalloven § 19 at dataansvarlig må sørge for at pasienters helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når det er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp. Tilgjengeliggjøringen av opplysninger om pasienter må skje innenfor rammene av taushetsplikten. Taushetsplikten er nærmere beskrevet i punktet om konfidensialitet.

Kravet om tilgjengeliggjøring etter pasientjournalloven § 19 er i stor grad den samme som etter helsepersonelloven § 45 og helsepersonelloven § 26 tredje ledd.

Ifølge helsepersonelloven § 45 skal helseopplysninger tilgjengeliggjøres for helsepersonell i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på en forsvarlig måte. Denne plikten gjelder tilgjengeliggjøring både internt i virksomheter og på tvers av virksomheter. Plikten etter helsepersonelloven § 45 gjelder imidlertid ikke dersom pasienten har motsatt seg slik tilgjengeliggjøring.

I helsepersonelloven § 26 tredje ledd er det krav om at den som yter helsehjelp, skal gi pasientens personnummer, opplysninger om diagnose, eventuelle hjelpebehov, tjenestetilbud, innskrivnings- og utskrivningsdato, samt relevante administrative data, til virksomhetens pasientadministrasjon.

Det er i pasientjournalloven § 19 og helsepersonelloven §§ 45 og 26 tredje ledd krav om å tilgjengeliggjøre helseopplysninger for annet helsepersonell. Det finnes også flere bestemmelser som gir mulighet for å tilgjengeliggjøre helseopplysninger på visse vilkår. Disse bestemmelsene er nærmere omtalt under punkt 1.5.3 om konfidensialitet.

## 1.5.3 Krav til konfidensialitet

Med «konfidensialitet» menes i Normen at helse- og personopplysninger må være sikret mot at uvedkommende får kjennskap til opplysningene.[3] Dette gjelder både uvedkomne internt i virksomheten og uvedkommende utenfor virksomheten. Kravet til konfidensialitet bør ses i sammenheng med taushetsplikten. 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. Taushetsplikt*

[2] Normen 6.0 vedlegg 6.2 Definisjoner
[3] Normen 6.0 vedlegg 6.2 Definisjoner

*innbefatter både en passiv plikt til å tie og en plikt til aktivt å hindre uvedkommende i å få kunnskap om taushetsbelagte opplysninger*.[4]

Helsepersonell og annet personell har taushetsplikt om det de får kjennskap til om pasientene under utøvelsen av sitt yrke.[5] Plikten gjelder for alle som får tilgang eller kjennskap til helseopplysninger, uavhengig av hvilken rolle vedkommende har overfor pasienten og for hvilket formål opplysningene behandles. Både opplysninger om helseforhold og andre personlige forhold er omfattet. Visse deler av sektoren er også underlagt taushetsplikt etter forvaltningsloven.[6] Virksomheter som yter helse- og omsorgstjenester skal organiseres slik at helsepersonell blir i stand til å overholde sine lovpålagte plikter, jf. helsepersonelloven § 16. Denne plikten kommer også til uttrykk i helse- og omsorgstjenesteloven § 4-1 og spesialisthelsetjenesteloven § 2-2.

Taushetsplikten er ikke absolutt. Unntak fra taushetsplikt må imidlertid følge av lov. Det er flere unntaksregler som tillater eller pålegger helsepersonell eller virksomheter som gir helsehjelp å gi tilgang til helseopplysninger. Reglene som pålegger helsepersonell eller virksomheter å gi tilgang, er omtalt under punkt 1.5.2 om tilgjengelighet. Det finnes imidlertid også regler som tillater tilgjengeliggjøring på visse vilkår. Slike regler finnes blant annet i helsepersonelloven §§ 25, 26 og 29 c.

Etter helsepersonelloven § 25 kan relevante og nødvendige opplysninger om en pasient gjøres tilgjengelig for personell som samarbeider om å yte helsehjelp til pasienten. Dette gjelder så lenge pasienten ikke har motsatt seg tilgjengeliggjøringen, og tilgjengeliggjøringen er nødvendig for å gi forsvarlig helsehjelp.

I helsepersonelloven § 26 første er det fastsatt at helseopplysninger kan deles med virksomhetens ledelse, dersom dette er nødvendig for å gi helsehjelp eller for internkontroll og kvalitetssikring. I bestemmelsens andre ledd fremgår det videre at slike opplysninger også kan deles med ledelsen i samarbeidene virksomhet, dersom det drives samarbeid om behandlingsrettede helseregistre etter pasientjournalloven § 9.

Det er på visse vilkår tillatt at opplysninger om pasienten gjøres tilgjengelig for helsepersonell som tidligere har gitt pasienten helsehjelp, jf. helsepersonelloven § 29 c. Tilgjengeliggjøringen kan skje dersom opplysningene er nødvendige for kvalitetssikring av helsehjelpen eller for helsepersonellets læring.

## 1.5.4 Krav til integritet

Med «integritet» menes i Normen at helse- og personopplysninger må være sikret mot utilsiktet eller uautorisert endring eller sletting.[7] Kravet til integritet bør ses i sammenheng med kravet til tilgangsstyring, som blant annet skal hindre at uautoriserte personer gjør endringer i helse- og personopplysninger.[8]

---

[4] Normen 6.0 vedlegg 6.2 Definisjoner

[5] Se blant annet helsepersonelloven § 21, pasientjournalloven § 15, helseregisterloven § 17 og helseforskningsloven § 7

[6] Jf. spesialisthelsetjenesteloven § 6-1 og helse- og omsorgstjenesteloven § 12-1, som bygger på den generelle taushetsplikten i forvaltningsloven §§ 13 til 13e

[7] Normen 6.0 vedlegg 6.2 Definisjoner.

[8] Det er viktig å være oppmerksom på at utilsiktet endring av opplysninger også kan oppstå som følge av feil i programvare, feil i integrasjoner, konfigurasjonsfeil eller konverteringsfeil når data overføres fra ett system til et

I særlovgivningen for helse- og omsorgssektoren kommer kravet til tilgangsstyring til uttrykk i pasientjournalloven § 22 og pasientjournalforskriften § 13. Pasientjournalforskriften § 13 første ledd stiller blant annet krav om at behandling av opplysninger i journal skal være basert på bestemte tillatelser til å redigere, rette, slette eller på annen måte behandle opplysninger i pasientjournal. Videre er det fastsatt i bestemmelsens tredje ledd at den dataansvarlige skal ha oversikt over hvem som har tilgang til hvilke typer opplysninger og kunne kontrollere i ettertid hvem som har benyttet seg av tilgangen.

Tiltak som er aktuelle for å ivareta opplysningers integritet vil ofte være de samme tiltakene som er aktuelle for å ivareta konfidensialitet. I begge tilfeller er det et ønske om å forhindre uautorisert tilgang til opplysningene.

### 1.5.5 Krav til gjennomføring av tilgangsstyring og systemkrav

I særlovgivningen for helse- og omsorgssektoren er det flere krav til hvordan tilgangsstyring skal etableres og gjennomføres i virksomheten.

Virksomheten må sikre at helsepersonell har tilgang til relevante og nødvendige helseopplysninger som er nødvendige for å gi helsehjelp, jf. pasientjournalloven § 19 og helsepersonelloven § 45. Samtidig må virksomheten sørge for å ivareta taushetsplikten, samt pasientens rett til å motsette seg tilgjengeliggjøring etter pasientjournalloven § 17, helsepersonelloven § 25 og pasient- og brukerrettighetsloven § 5-3. Det stilles derfor krav i pasientjournalloven § 7 om at virksomheten må sørge for at systemene som benyttes for behandlingsrettet helseregister er utformet og organisert slik at disse kravene kan etterleves.

I pasientjournalloven § 22 er det krav om at virksomheten skal sørge for tilgangsstyring i behandlingsrettet helseregister. Bestemmelsen stiller ingen konkrete krav til hvordan tilgangsstyring skal etableres og gjennomføres, men at virksomheten må ha en risikobasert tilnærming ved iverksetting av tiltak som tilgangsstyring. I pasientjournalforskriften er det imidlertid gitt noen mer konkrete krav til autorisering, autentisering og logging i pasientjournal, jf. §§ 13 og 14, samt at dataansvarlig skal ha kontroll og oversikt over bl.a. tilgjengeliggjøring av opplysninger til andre virksomheter, jf. § 12 tredje ledd.

Av pasientjournalforskriften § 14 annet ledd følger det at pasienten har rett til å få innsyn i loggene som viser hvem som har skaffet seg tilgang til pasientens helseopplysninger og hvem som har mottatt disse. Videre følger det av pasientjournalloven § 25 at helseopplysninger skal oppbevares så lenge det er nødvendig av hensyn til helsehjelpens karakter, og at det samme gjelder for loggene over hvem som har fått utlevert helseopplysninger som er knyttet til pasientens navn eller fødselsnummer.

### 1.5.6 Standarder og rammeverk

I tillegg til at veilederen legger til grunn relevante lover og forskriftsbestemmelser, bygger veilederen på flere standarder og rammeverk for beste praksis innen tilgangsstyring. Særlig

annet eller fra ett format til et annet. Kravet til integritet bør derfor også ses i sammenheng med krav som skal hindre slik endring. Slike krav finnes i Normen 6.0, Kapittel 5.4.1 Konfigurasjonskontroll og kapittel 5.4.2 Endringsstyring.

relevante standarder og rammeverk er ISO/IEC 27002[9], NSMs grunnprinsipper for IKT-sikkerhet 2.0[10] og Centre for Internet Security (CIS) Controls v 8[11].

## 1.6 Avgrensninger

Denne veilederen er avgrenset til tilgangsstyring i behandlingsrettede helseregistre som skal gi grunnlag for helsehjelp eller å administrere eller kvalitetssikre helsehjelp. Veilederen dekker både tilgangsstyring for helsepersonell og annet personell, herunder administrativt personell, driftspersonell og annet personell som gis tilgang til den underliggende IKT-infrastrukturen for behandlingsrettet helseregister. Veilederen gjelder ikke tilgangsstyring for andre formål, som for eksempel i forbindelse med forskning.[12] Det er utarbeidet et eget veiledningsmateriell for forskning, der tilgangsstyring blir omtalt.[13]

Veilederen er ment å gi en praktisk tilnærming til konkrete problemstillinger innenfor området tilgangsstyring, men vil ikke nødvendigvis gi svar på alle spørsmål som kan dukke opp i praksis. Når anbefalingene i veilederen tas i bruk i virksomheten, må de tilpasses med utgangspunkt i virksomhetens kompleksitet og størrelse, samt konkrete behov og oppgaver.

Temaer som kan være relevant i forbindelse med etablering av tilfredsstillende tilgangsstyring, men som er omtalt i andre veiledere eller i annet veiledningsmateriell, vil ikke bli omtalt i detalj i denne veilederen. For slike temaer vil det istedenfor henvises til relevant veiledningsmateriell. Det er av denne grunn ikke en egen omtale av temaer som omhandler for eksempel tilgangsstyring til skyløsninger og portalløsninger, samt velferdsteknologi, IoT eller fjernaksess fra leverandør.

Videre vil veilederen ikke inkludere de mer tekniske og teknologispesifikke aspektene ved tilgangsstyring, da veilederen er ment å ha en praktisk tilnærming i sektoren.

[9] I ISO/IEC 27002 er særlig områdene A9 Aksesskontroll og A12.4 Logging og overvåking relevante
[10] NSM – Grunnprinsipper for IKT-sikkerhet 2.0
[11] CIS Controls: https://www.cisecurity.org/controls/ - Tilgang til kontrollene er gratis, men krever registrering. Særlig områdene 5 – Account Management, 6 – Access Management og 8 – Audit log management er relevante
[12] For å få tilgang til helse- og personopplysninger for forskningsformål må det sendes søknad til Regionale komiteer for medisinsk og helsefaglig forskningsetikk (REK). Eventuell tilgang vil dermed følge av søknaden.
[13] Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren

# 2. Generelle prinsipper for tilgangsstyring

## 2.1 Hva er tilgangsstyring?

Tilgangsstyring er et sett med regler for å styre hvem som skal ha tilgang til hvilke opplysninger eller systemer.[14] Tilgangsstyring har som formål å gi personell med tjenstlig behov tilgang til opplysninger eller informasjonssystemer, samtidig som uautoriserte blir hindret tilgang til opplysninger eller informasjonssystemer. Formålet med tilgangsstyring er altså ikke bare det å begrense personers tilgang til opplysninger og informasjonssystemer, men vel så mye å sikre at personell får de riktige tilgangene til riktig tid og av riktig grunn.

Å etablere et sett med regler for tilgangsstyring i en virksomhet, som fullt ut dekker alle behov og situasjoner, er utfordrende og nærmest umulig. Det er derfor viktig at reglene som etableres er forholdsmessige og basert på risikovurderinger (se kapittel 2.4 og 2.5). At det er etablert en tilfredsstillende tilgangsstyring i virksomheten, er en forutsetning for å oppnå forsvarlig sikkerhet. Dette oppnås gjennom en helhetlig tilnærming, der både teknologiske og organisatoriske sikkerhetstiltak spiller inn.

Tilfredsstillende tilgangsstyring forutsetter at virksomheten har gode rutiner for hvordan tilganger skal etableres, endres og avsluttes, og har identifisert hvilke sikkerhetstiltak som må være implementert hos virksomheten og i hele verdikjeden for informasjonssystemet. Dette kan for eksempel være rutiner og sikkerhetstiltak knyttet til administrative og operasjonelle prosesser, sikkerhetsstyring, personellsikkerhet, fysisk sikkerhet og adgangskontroll, opplæring og bevisstgjøring, design av IKT-arkitekturen og teknologivalg.

Tilgangsstyring er et vesentlig virkemiddel for å ivareta kravet til konfidensialitet, integritet og tilgjengelighet.

**Konfidensialitet** – sikre at helse- og personopplysninger er beskyttet mot at uvedkommende får kjennskap til opplysningene. Konfidensialitet bidrar til ivaretakelse av taushetsplikt og personvern.

**Integritet** – sikre at helse- og personopplysninger er beskyttet mot utilsiktet eller uautorisert endring eller sletting. Opplysningene skal være korrekte og om nødvendig oppdaterte, og kopier av data skal ikke bli en kilde til utdatert informasjon.

**Tilgjengelighet** - sikre at helse- og personopplysninger som skal behandles, er tilgjengelig for personell med tjenstlig behov til den tid og på det sted det er behov for opplysningene.

[14] Datatilsynet - https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/#T

## 2.2 Tilgangsstyring i helse- og omsorgsektoren

Virksomheter i helse og omsorgssektoren skal i henhold til Normen ha rutiner for autorisering, endring og avslutning av tilganger.[15] Tilgangsstyring handler om hvordan virksomheten gjennomfører

- autorisering for tilgang til informasjonssystemer
- autorisering for tilgang til behandlingsrettet helseregister, som innebærer tildeling av tillatelser til å kunne lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger
- autentisering, som sikrer identifisering av autorisert bruker
- tilgjengeliggjøring av helse- og personopplysninger om bestemte pasienter for autorisert personell i egen virksomhet, herunder også driftspersonell og annet personell med tjenstlig behov
- tilgjengeliggjøring av helse- og personopplysninger til samarbeidende personell i andre virksomheter
- kontrollerende tiltak.

Kravene til tilgangsstyring gjelder uavhengig av hvilken teknisk løsning som ligger til grunn. Kravene er derfor ikke begrenset til kun å gjelde EPJ-systemer inkludert fagsystemer med lokal autentiseringsløsning. Enkelte virksomheter har et påloggingssystem som kan benyttes i flere ulike tjenester («single sign-on») for autentisering til helse- og personopplysninger, og da vil det være vel så viktig å sikre en tilfredsstillende tilgangsstyring til den underliggende IKT-infrastrukturen.

Virksomheten skal sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og samarbeidende personell i andre virksomheter, når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte. Virksomheten bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige for andre virksomheter, men tilgjengeliggjøring skal skje på en måte som ivaretar taushetsplikten, informasjonssikkerheten og personvernet.[16]

Tilgang til behandlingsrettede helseregistre skal gis etter en konkret beslutning basert på om det er eller skal etableres tiltak for helsehjelp til pasienten. Tilgangen skal styres slik at reglene om taushetsplikt ivaretas, og at tilgang til helse- og personopplysninger kun gis til personell med tjenstlig behov.[17]

## 2.3 Tilgang til relevante og nødvendige opplysninger

Helsepersonell skal gis tilgang til relevante og nødvendige helseopplysninger, i den grad det er nødvendig for å kunne gi helsehjelp til pasienten på en forsvarlig måte.[18] Relevante og nødvendige opplysninger vil for eksempel være de opplysningene som det i den aktuelle undersøkelses- og behandlingssituasjonen er behov for å ha tilgjengelig, for å kunne yte

[15] Normen 6.0 kapittel 5.2 Tilgangsstyring
[16] Les mer om tilgang mellom virksomheter i kapittel 71.5.
[17] Normen 6.0 kapittel 5.2 Tilgangsstyring
[18] Helsepersonelloven § 45

forsvarlig helsehjelp. Relevante og nødvendige opplysninger kan også være opplysninger det kan bli aktuelt å hente fram i forbindelse med helsehjelp som ytes på et senere tidspunkt. Oftest må personellet selv vurdere hvilke helseopplysninger som er relevante og nødvendige. Dette kan være opplysninger som ikke alltid er dekket av den tildelte tilgangen og som det derfor kan være vanskelig å identifisere behov for tilgang til i forkant. For å sikre tilstrekkelig og rettidig tilgang i slike tilfeller, kan for eksempel selvautorisering benyttes. Ved etablering av tilgangsstyringen må behovet for selvautorisering vurderes slik at virksomheten tilrettelegger for at helsepersonell får de nødvendige tilgangene. Les mer om selvautorisering i kapittel 3.6.

Helsepersonell er gjennom dokumentasjonsplikten pålagt å dokumentere relevante og nødvendige opplysninger om pasienten. Formålet med denne dokumentasjonsplikten er å understøtte pasientsikkerheten, ved å sikre at opplysninger som er nødvendige og relevante for en forsvarlig behandling av pasienten blir nedtegnet og kan gjenfinnes.

## 2.4 Forholdsmessighet

Etableringen av sikkerhetstiltak knyttet til tilgangsstyring skal, som øvrige sikkerhetstiltak, baseres på forholdsmessighet.[19] Forholdsmessighet innebærer at omkostningene med tiltak skal stå i et rimelig forhold til hva som oppnås med tiltakene. Omkostninger kan være redusert pasientsikkerhet, økte økonomiske utgifter eller inngrep i personvernet. I enkelte situasjoner, som for eksempel ved systemovervåking og kontroll av brukere, kan økt personvern for noen personer (for eksempel pasienter) oppnås ved å gjøre inngrep i andres personvern (for eksempel helsepersonell). Også da må avveininger gjøres for å oppnå forholdsmessighet.

Ved etablering av tilgangsstyring skal virksomheten vurdere hva som er forholdsmessig ut fra virksomhetens størrelse, kompleksitet, art og omfang av behandling av helse- og personopplysninger, pasientsikkerhet og risikobildet. Dette kan for eksempel bety at større og mer komplekse virksomheter som behandler et stort omfang av helse- og personopplysninger, kan være nødt til å etablere flere tiltak enn mindre virksomheter som behandler helse- og personopplysninger i mindre omfang, og der risikoen er mindre kompleks og lettere håndterbar. Det er imidlertid viktig å poengtere at pasientens rettighet til god sikkerhet ikke under noen omstendighet skal gå på bekostning av forholdsmessighet knyttet til virksomhetens størrelse. De tekniske tiltakene som ligger til grunn for god tilgangsstyring bør derfor være på samme sikkerhetsnivå uavhengig av virksomhetens størrelse. Når det gjelder organisatoriske tiltak, kan det være aktuelt for større og mer komplekse virksomheter å iverksette flere og annerledes tiltak enn mindre komplekse virksomheter. Organisatoriske tiltak kan kompensere noe for nivået på digitale eller fysiske tekniske tiltak. For å oppnå akseptabel risiko, kan det implementeres risikoreduserende administrative tiltak i form av rutiner og menneskelige tiltak i form av opplæring, for eksempel dersom planlagte tekniske tiltak ikke kan innføres umiddelbart.[20]

Et viktig grunnlag for å kunne vurdere forholdsmessighet, er å vurdere risiko. I neste kapittel omtales risikovurdering.

[19] Normen 6.0 kapittel 1.5 Om Normens krav og kapittel 3.1 Forholdsmessighet ved valg av tiltak
[20] Normen 6.0 kapittel 3.4 Risikovurdering og risikohåndtering

## 2.5 Risikovurdering

### 2.5.1 Om risikovurdering og relevansen for tilgang

Risikostyring er koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko. Det omfatter å få oversikt over informasjon og teknologi i virksomheten, identifisere trusler og mulige uønskede hendelser for både virksomheten og de registrerte, analysere risikoen og etablere tiltak for å opprettholde nivå for akseptabel risiko.[21]

Valg av løsning for tilgangsstyring skal baseres på en risikovurdering. Risikovurderingen skal dokumenteres.[22] I henhold til Normen skal tekniske og organisatoriske tiltak etableres for å håndtere identifisert risiko på en tilfredsstillende måte. Virksomhetens valg av egnede tekniske og organisatoriske tiltak skal vurderes opp mot forholdsmessigheten. Dette gjelder særlig i vurderingen av egnet sikkerhetsorganisasjon, arbeidsoppgaver, kontrolloppgaver og tiltak innen tilgangsstyring.

Virksomheten er pålagt å fastsette nivå for akseptabel risiko basert på Normens minimumskrav til informasjonssikkerhet og eventuelt egne infromasjonssikkerhetsmål. Videre skal virksomheten, gjennom egnede sikkerhetstiltak, sikre at restrisikoen er akseptabel. Normen stiller følgende overordnede minimumskrav til informasjonssikkerhet som har direkte tilknytning til temaet tilgangsstyring (konfidensialitet, integritet, tilgjengelighet og robusthet):[23]

**Minimumskrav for å sikre konfidensialitet**

Virksomheten skal ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysninger, ved å

- hindre uautorisert tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten
- avgrense tilgang for autorisert personell iht. tjenstlig behov
- ha oversikt (logger) over alle som har hatt tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten.

> Et av hovedtiltakene for å sikre konfidensialitet er å implementere gode og effektive tiltak for tilgangsstyring. Eksempler på dette vil løpende bli redegjort for i veilederen.

**Minimumskrav for å sikre integritet**

Virksomheten skal sikre integriteten til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten, ved å

- logge hvem som har rettet, registrert, endret og slettet opplysningene
- hindre utilsiktet eller uautorisert endring eller sletting av opplysningene.

[21] Normen 6.0 kapittel 3. Risikostyring
[22] Normen 6.0 kapittel 3.4 Risikovurdering og risikohåndtering
[23] Normen 6.0 kapittel 3.2 Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet

Et eksempel på et tiltak virksomheten kan iverksette for å hindre uautorisert endring eller sletting, er å sperre for endring av data som ikke skal endres, som for eksempel prøvesvar, registrerte målinger og undersøkelsesresultater, autorisasjonsregister og logger.

**Minimumskrav for å sikre tilgjengelighet og robusthet**

Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er tilgjengelig til rett tid, ved å

- sikre at helse- og personopplysninger er tilgjengelig iht. tjenstlig behov.

Sett ut fra et tilgangsstyringsperspektiv innebærer dette å sikre at personell gis de nødvendige autorisasjonene for å yte forsvarlig helsehjelp, og sikre at disse er i tråd med tjenstlig behov.

## 2.5.2 Praktiske råd om risikovurderinger

Det er utarbeidet et eget veiledningsmateriell for Normen som går i dybden på hvordan risikovurderinger bør gjennomføres i praksis.[24] Dette kapitlet tar for seg konkrete eksempler knyttet til tilgangsstyring. Forhold knyttet til risikovurderinger blir også løpende diskutert i de ulike kapitlene i veilederen.

I Normen er det krav om at risikovurderinger skal gjennomføres når det er nødvendig, men det er også noen minimumskrav for når risikovurderinger skal gjennomføres.[25] I tekstboksen under har vi oppsummert de kravene til risikovurdering som kan knyttes direkte til tilgangsstyring.

Risikovurdering skal ligge til grunn for

- valg av sikkerhetstiltak i forbindelse med tilgangsstyring internt i virksomheten
- etablering eller endring av tilgang til helseopplysninger mellom virksomheter
- bruk og tildeling av administratorbrukere
- valg av sikker metode for autentisering
- tilgang via mobilt utstyr og fjerntilgang.

Risikovurderinger bør være scenariobasert og ta utgangspunkt i uønskede hendelser som kan oppstå i virksomheten. I forberedelsene til risikovurderingen bør det utarbeides forslag til uønskede hendelser som tas med inn i risikovurderingen.

[24] Veileder i risikostyring i helse- og omsorgssektoren

[25] Normen 6.0 kapittel 5 Informasjonssikkerhet, 5.2.1 Autorisering, 5.2.1.2 Tilgang til helse- og personopplysninger mellom virksomheter, 5.2.2 Autentisering og 5.3.4 Mobilt utstyr og hjemmekontor

***Eksempel på scenarioer som er relevant for tilgangsstyring:***

- Ansatte får ikke tilgang til systemene og applikasjonene de trenger for å yte helsehjelp
- Ansatte får tilgang utover tjenstlig behov som kan føre til:
  - Uautorisert tilgang til helse- og personopplysninger
  - Utilsiktet endring eller sletting av helse- og personopplysninger
- Eksterne uvedkommende bryter seg inn i systemene og får tilgang til helse- og personopplysninger
- Ansatte lar PCer og applikasjoner stå åpne og tilgjengelige for andre når de går fra PCen
- Utlevering av autentiseringsfaktorer (som ID-kort, smartkort, påloggingsinformasjon) skjer til feil person

Når selve risikovurderingen skal gjennomføres bør det etableres en arbeidsgruppe som består av representanter fra ulike deler av virksomheten, slik at man sikrer at ulike perspektiv blir vurdert og tatt stilling til. Arbeidsgruppen bør bestå av personer med sikkerhetskompetanse, personvernkompetanse, IKT- og systemkompetanse og juridisk kompetanse, samt brukere av systemene (helsepersonell), og hvis relevant også pasientrepresentanter (som for eksempel brukerutvalg). Det er særlig relevant å involvere helsepersonell i risikovurderinger innen tilgangsstyring. Grunnen til dette er at de både er daglige brukere av systemene og kjenner til relevante problemstillinger som kan oppstå daglig, samt at de også kjenner til de helsefaglige konsekvensene som er viktig å ta med i risikovurderingen. For å muliggjøre deltakelse fra helsepersonell er det viktig med god planlegging for å legge opp til en gjennomføring utenfor helsepersonellets kjernetid.

Etter gjennomført risikovurdering bør beslutninger om sikkerhetstiltak for tilgangsstyring tas av personell på ledernivå med kompetanse til å vurdere både forsvarlig pasientbehandling og informasjonssikkerhet. Personell som tar denne beslutningen, er også eier av risikoen. Virksomheten bør overvåke restrisiko i perioden etter at en risikovurdering er gjennomført. Det bør utarbeides en rutine for å gjennomgå tidligere risikovurderinger, og oppdatere disse ved endringer i risikobildet, ved nye relevante problemstillinger og etter implementering av risikoreduserende tiltak. For eksempel bør risikovurderingen oppdateres dersom det er ønske om å gjøre endringer i tilgangsrettigheter til en gruppe helsepersonell/gitt rolle i systemet, før større programendringer og versjonsoppgraderinger av betydning for tekniske tiltak for tilgang, og etter hvert som avvik fra tilgangsrutinene oppdages og håndteres.

# 3. Autorisering

## 3.1 Generelt om autorisering

Autorisering for tilgang til helse- og personopplysninger innebærer tildeling av rettigheter til å kunne lese, registrere (inklusive rekvirere, signere og kontrasignere), redigere, rette, slette eller sperre helse- og personopplysninger. Autorisasjon kan gis gjennom systemtilganger med disse rettighetene. Eksempler på informasjonssystem og data som personell autoriseres for kan være fagsystemer, helseregistre eller journaler med helseopplysninger om pasienter og brukere. Andre eksempler er systemer og databaser med opplysninger om personalet, legemidler eller helseberedskapen i virksomheten.

Autorisasjon skal bare gis i den grad det er nødvendig ut ifra tjenstlig behov og så langt lovbestemt taushetsplikt ikke er til hinder for det. Dataansvarlig er ansvarlig for at autorisasjon for tilgang tildeles, administreres og kontrolleres, og kan ved behov delegere myndighet til ledere for den enkelte enhet. I dette ligger at leder, innen eget ansvarsområde, skal vurdere og godkjenne personellets behov for å få tilgang til helse- og personopplysninger. Det er ikke uvanlig at ledere for den enkelte enhet, i samråd med lederen som er gitt ansvar for systemet eller dataene autorisasjonen gjelder, gir tillatelse og ivaretar ansvaret for tildeling av tilganger. Tildeling av tilgang bør være dokumentert og det bør foreligge sporbarhet om hvem som har gitt autorisasjonen.

For personell med flere roller i virksomheten, skal autorisering skje for hver rolle, uavhengig av vedkommendes øvrige roller.[26] Dette gjelder spesifikt for de virksomhetene som benytter roller i reglene de lager for tilgangsstyring (se kapittel 3.3 om rollebasert tilgang). Hvilken autorisasjon for tilgang som skal gis i en virksomhet skal være tilpasset risikoen ved behandling av helse- og personopplysninger. Større virksomheter og virksomheter med særlig følsomme opplysninger vil gjerne ha flere og tydelige atskilte funksjoner og kan gi personell autorisasjon ut ifra hvilken funksjon de fyller (rollebasert). For små virksomheter der det for eksempel bare er to-tre personer, kan etablering av mange ulike roller bli mer komplekst og ressurskrevende enn nødvendig.

Autorisasjonene for tilganger skal bidra til å sikre en tilfredsstillende informasjonssikkerhet. Informasjonssikkerheten skal vurderes helhetlig og ikke ut fra autorisasjonssystemet alene. Dette innebærer at øvrige sikkerhetstiltak som logging, innsyn i logger og loggoppfølging også er komponenter som skal bidra til å oppnå tilfredsstillende informasjonssikkerhet.

For å hindre uautorisert tilgang skal det ifølge Normen etableres følgende tiltak:

- Dersom det er åpnet for selvautorisering, skal tilgang grunngis og registreres.
- Tekniske tiltak skal sikre at personer i eller utenfor virksomheten ikke skal kunne endre opplysninger uten at det registreres i informasjonssystemene hvem som har endret, og hva som er endret.
- All tildeling av autorisasjon skal registreres i et autorisasjonsregister.
- Tekniske tiltak skal også sikre at personer i eller utenfor virksomheten ikke skal kunne endre konfigurasjon og programvare uten at det logges.
- Risikovurdering skal begrunne behovet for ulike administratorbrukere.
- Personell med administratortilganger skal benytte personlig separat brukerkonto for administratoroppgaver. Driftspersonell skal ha personlige brukerkontoer for oppgaver som ikke krever administratortilganger.

Det siste kulepunktet i listen er tydelig på at det skal benyttes separate brukerkontoer for administratoroppgaver. Det eksisterer enkelte løsninger for tilgangsstyring som ivaretar intensjonen til dette kravet, men som håndterer brukere på litt annen måte. Et eksempel på dette er bruk av PAM[27] for styring av administratortilganger. I slike tilfeller kan det være mest

[26] Normen 6.0 kapittel 5.2.1 Autorisering

[27] PAM står for «privileged access management» og er en løsning som benyttes for å håndtere og styre bruken av privilegerte brukerkontoer.

hensiktsmessig at brukeren benytter sin ordinære brukerkonto for å logge på PAM, og at det i PAM er regulert hvilke administratortilganger den enkelte er autorisert for å benytte seg av. Risikoen tilknyttet bruk av administratorbrukere, som kravet har til intensjon å dekke, blir da ivaretatt, og det vurderes at kravet derfor oppfylles ved bruk av en slik løsning.

## 3.2 Tjenstlig behov for tilgang til helse- og personopplysninger

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 og kvalitetssikring i forbindelse med dette.[28] Det finnes flere ulike typer tjenstlig behov for tilgang til helse- og personopplysninger, og i dette kapitlet tar vi for oss noen eksempler.

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

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[29]. Det er ingen konkrete krav om å benytte en bestemt modell for å dokumentere beslutningen, som for eksempel beslutningsstyrt tilgang. Det er imidlertid et krav om å dokumentere helsehjelpen som er gitt, og at beslutningen om å yte helsehjelp da implisitt dokumenteres. Dette gjelder også for tilgang i ordinære akuttsituasjoner, som ikke er å regne som selvautorisering (se kapittel 3.6).

Kommunen skal sørge for at personer som oppholder seg i kommunen tilbys nødvendige helse- og omsorgstjenester. Ulike grupper helse- og omsorgspersonell vil være delaktig i ytelsen av omsorgtjenester i kommunene, og disse vil ha behov for tilgang til relevante helseopplysninger for å levere nødvendige og korrekte tjenester. For eksempel vil lege, sykepleier, fysioterapeut, jordmor, helsesykepleier, vernepleier, ergoterapeut og psykolog ha behov for opplysninger om pasienten. Personell som ikke er helsepersonell, som for eksempel støttekontakter og hjemmehjelper, vil derimot ikke ha det samme behovet for slik tilgang.

**Administrasjon av helsehjelp**
Personell som utfører oppgaver knyttet til administrasjon av helsehjelp er ikke alltid helsepersonell, men må likevel ha tilgang til helseopplysninger for å kunne utføre sitt arbeid.

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)

[28] Normen 6.0 vedlegg 6.2 Definisjoner
[29] Normen 6.0 kapittel 5.2 Tilgangsstyring

- pasientkoordinering (for eksempel kontroll av at helsehjelpen/tjenesten er levert til pasienten/brukeren)
- fordeling av hjemmebesøk.

Ved tildeling av autorisasjon for tilgang skal behovet for tilgang vurderes opp mot 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.

**Teknisk drift og forvaltning**
Med teknisk personell menes her medarbeidere som jobber med drift av teknisk løsning eller forvaltning av elektronisk pasientjournal eller fagsystemer. Gjennom sitt arbeid kan IKT-personell ha behov for tilgang til større mengder 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 skal til enhver tid være sporbart hvem som har utført ulike handlinger i systemet. I tilfeller der det ikke er mulig å benytte personlige brukere, skal det loggføres hvem som til enhver tid har benyttet seg av fellesbrukeren. Dette kan for eksempel gjøres gjennom at tilgang gis via en PAM-løsning (se fotnote 29) basert på personlige brukere som er autorisert for å benytte fellesbrukeren.

**Kvalitetssikring**
Helseopplysninger kan gjøres tilgjengelig i forbindelse med kvalitetssikring og skal begrenses til de opplysninger som er relevante og nødvendige 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.

## 3.3 Ulike prinsipper for tilgang

**Beslutningsstyrt tilgang**

Beslutningsstyrt tilgang kan benyttes for å gi tilgang til helse- og personopplysninger[30]. En registrert beslutning om ytelse av helsehjelp vil være grunnlaget for at personell som skal delta i ytelsen av helsehjelpen får tilgang til å åpne pasientens journal. Slik tilgang vil ofte kunne gis implisitt, for eksempel som en følge av at en beslutning om innleggelse til en bestemt form for behandling registreres i en journal på et sykehus. Et annet eksempel er når det i den journalen som pleie- og omsorgstjenesten fører, registreres at pasienten har takket ja til et tilbud om sykehjemsplass.

Beslutningsstyrt tilgang benyttes ikke bare dersom det foreligger en beslutning om ytelse av helsehjelp. Et tredje eksempel på beslutningsstyrt tilgang er ved mottak av en henvisning, der helsepersonell som er tildelt oppgaven med å vurdere henvisningen vil ha behov for å gjøre oppslag i pasientens journal. Resultatet av vurderingen vil i noen tilfeller være at forespørselen om helsehjelp avvises og at det ikke besluttes å iverksette behandling.

Videre kan prinsippene for beslutningsstyrt tilgang også benyttes ved administrasjon av helsehjelp. Personell som utfører administrasjon av helsehjelp, skal uten hinder av taushetsplikten gis pasientens fødselsnummer og opplysninger om diagnose, eventuelle

[30] EPJ standard: Tilgangsstyring, retting og sletting - kapittel 2

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 3.4).

Tilgang i journalsystem eller fagsystem kan styres automatisk i forbindelse med ytelse av helsehjelpen, ved at det gis et tidsvindu for når tilgangen er åpen. Det vil si at journalen/fagsystemet kan åpnes i henhold til autorisasjonen for tilgang, for personell som er autorisert og 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.

**Rollebasert tilgang**

Bruk av roller er en modell som kan benyttes i regler for tilgangsstyring når dette anses hensiktsmessig. Med rolle menes en kategorisering av personell som vil kunne yte, administrere eller kvalitetssikre helsehjelpen til pasienten/brukeren. Rolle kan også knyttes til en organisatorisk enhet. Bruk av roller er effektivt for dokumentasjonshensyn, ved at det er tydelig hvilken funksjon den som har aksessert opplysninger har hatt på tidspunktet opplysningene ble aksessert.

Rettigheter til å lese, registrere, redigere og rette helseopplysninger i rollene fastsettes ut fra informasjonsbehovet og dokumentasjonsplikten ulike grupper ansatte vil ha ved ytelse av helsehjelpen. Rettighetene kan administreres i en rollemal som beskriver hvilke tilganger de som opptrer i rollen skal ha, og hvilken journalinformasjon de som innehar rollen normalt skal gis tilgang til når det ytes helsehjelp.

Rollebasert tilgangsstyring er spesielt relevant å benytte når samme bruker gjennom ulike funksjoner har ulike tilgangsbehov. Tilgangen styres da ved å tildele personen flere roller i journalsystemet eller fagsystemet. Hver rolle skal tildeles selvstendig, uavhengig av vedkommendes øvrige roller, og ved behov gis ulike autentiseringsfaktorer.

Det er viktig å merke seg at det å operere med flere forskjellige roller for samme person kan by på utfordringer. Dette da helsepersonell kan ha behov for å opptre i flere roller i løpet av en arbeidsøkt, og det da kan være krevende å måtte bytte roller underveis i økten. Roller som knyttes til lokasjoner vil også kunne gi utfordringer, for eksempel der en sykehusavdeling har filialer på ulike geografiske steder og hvor leger ambulerer mellom stedene. For eksempel vil laboratoriesvar ofte måtte følges opp i ettertid når legen befinner seg på en annen lokasjon enn der prøven ble tatt. Den aktuelle rollen knyttet til denne lokasjonen gir ikke nødvendigvis tilgang til journalen til de pasientene legen trenger å følge opp på en annen lokasjon.

Det er ikke uvanlig at helsepersonell bruker mye tid på bytte av roller under en arbeidsdag, og det er ikke alltid tydelig hvilke tilganger som ligger i de ulike rollene. Det kan innebære at helsepersonell må «prøve og feile» før nødvendig tilgang oppnås. Det kan derfor være fristende for helsepersonell å benytte seg av den rollen som gir bredest tilgang, uavhengig av hvilken funksjon brukeren er satt til å fylle i hver enkelt situasjon. Dette for å bruke minst mulig tid på å få tilgang til de pasientjournalene de har tjenstlig behov for tilgang til. Tilstrekkelig opplæring i hva de ulike rollene gir tilgang til vil kunne avhjelpe dette problemet noe. Videre vil det være aktuelt å inkludere utfordringen med bruk av flere roller i risikovurderinger, da dette kan gå ut over effektivitet og i verste fall begrense helsepersonellet i å yte forsvarlig helsehjelp.

Behovet for roller og detaljstyring av tilgang for den enkelte rolle avhenger av virksomhetens størrelse og organisering.

***Eksempel:***
Roller kan utarbeides med utgangspunkt i brukernes ulike funksjoner og tilhørighet i virksomheten.

| Eksempel på roller |
|---|
| Lege ved anestesiavdelingen |
| Sykepleier ved sengepost A7 |
| Lege ved medisinsk avdeling |
| Vakthavende lege |
| Kontormedarbeider / resepsjonist |
| IT-personell |

| Eksempel på rollemaler |
|---|
| Lege |
| Sykepleier |
| Fysioterapeut |
| Jordmor |
| Helsesekretær |
| IT-funksjon |

## 3.4 Autorisasjonsregister

Alle tildelte autorisasjoner for tilgang skal registreres i et autorisasjonsregister.[31] Dette gjelder ikke bare for helsepersonell, men også annet personell med tilgang til helse- og personopplysninger, som for eksempel teknisk personell. Det er virksomheten som skal sørge for at det opprettes et autorisasjonsregister. Registeret skal sikres mot uautorisert endring og sletting.

Autorisasjonsregisteret skal som minimum inneholde[32]

- informasjon om hvem som er tildelt autorisasjon (entydig identifikator, men helst ikke direkte bruk av fødselsnummer)
- informasjon om til hvilken rolle autorisasjonen er tildelt (om roller benyttes i virksomheten)
- formålet med autorisasjonen
- tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt
- informasjon om hvilken virksomhet den autoriserte er knyttet til
- helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet (kun om tilgang til helseopplysninger i annen virksomhet er tatt i bruk).

I tillegg til punktene over anbefales det at autorisasjonsregisteret også inneholder navn og entydig identifikator til den som har registrert og tildelt/endret autorisasjonen.

Autorisasjonsregister kan opprettes med for eksempel

- funksjonalitet i journalsystemet eller fagsystemet
- brukerlister fra journalsystemet eller fagsystemet som lagrer historikk på opprettelse, endring og deaktivering av autorisasjon for tilgang
- regneark
- tekstdokument
- løsning for identitetsregister (f.eks. IDM-/IAM-løsninger).

[31] Pasientjournalforskriften § 13 første ledd bokstav c
[32] Normen 6.0 kapittel 5.2.1.1 Autorisasjonsregister

Under følger to eksempler på hvordan en helsevirksomhet kan føre og vedlikeholde et autorisasjonsregister i praksis. Det første eksempelet tar for seg manuell føring av autorisasjonsregisteret, og det andre eksempelet tar for seg en automatisert prosess.

***Eksempel på et manuelt ført autorisasjonsregister:***

Normsund legekontor er et lite legekontor som består av 5 praktiserende leger og en helsesekretær. Line, en av de fem legene, er også daglig leder av legekontoret og er ansvarlig for å sikre etterlevelse av de krav som stilles til autorisasjonsprosessen. Det er Line selv som autoriserer legekontorets helsepersonell, men den operative oppgaven med å registrere og vedlikeholde autorisasjonsregisteret har hun delegert til legekontorets sekretær.

Ettersom legekontoret har en håndterbar mengde ansatte og et mindre komplekst IT-miljø, har legekontoret besluttet at autorisasjonsregisteret skal føres manuelt. Det er opprettet et eget regneark som benyttes for å registrere og vedlikeholde autorisasjonene. Regnearket er tilgangsstyrt og det er kun Line og legekontorets sekretær som har tilgang til å gjøre endringer i dokumentet. De endringene som gjøres logges i dokumentets versjonshistorikk.

Selv om legekontoret er lite og alle kjenner alle, er det formalisert en rutine for tildeling eller endring av autorisasjon. Rutinen skal sikre at bestillinger skjer skriftlig og kan ettergås ved behov. Ved tildeling eller endring av autorisasjon sender Line en e-post til helsesekretæren med opplysninger om ansettelsesforholdet, herunder stilling, varighet og hvilke tilganger den ansatte skal ha. Sekretæren lagrer e-posten i en egen mappe for tilgangsbestillinger og oppdaterer autorisasjonsregisteret i tråd med bestillingen fra Line.

***Eksempel på et automatisk ført autorisasjonsregister:***

Normland helsesenter er et middels stort helsesenter som består av 40 ansatte med ulik helsefaglig bakgrunn, samt 5 ansatte i støttefunksjoner knyttet til IT og økonomi.

Autorisasjonsregisteret til Normland er integrert mot «service management»-systemet som driftes av IT-avdelingen. «Service management»-systemet benyttes blant annet for brukeradministrasjon og bestilling av tilganger til informasjonssystemene. Dersom det er behov for å opprette ny bruker, eller gjøre endringer i en brukers tilganger, meldes dette inn til IT via «service management»-systemet. Dette gjelder for alle tilganger til virksomhetens IKT-infrastruktur og informasjonssystemer. Normland har definert at det er den ansattes overordnede leder som er autorisert til å gjøre slike bestillinger.

Når bestillingen er registrert og brukeren er gitt tilgang til behandlingsrettede helseregistre, oppdateres autorisasjonsregisteret automatisk. Behovet for autorisasjonen fremkommer av den ansattes engasjement, rolle og organisasjonstilhørighet. Autorisasjonsregisteret inneholder da både informasjon om den autoriserte og informasjon om hvem som har autorisert tilgangen. I tilfeller der personell autoriseres for tilganger utover definerte standardtilganger, er det krav til at bestiller legger inn en kommentar som begrunner behovet og varigheten for tilgangen.

Dersom autorisasjonsregisteret er en separat oversikt, og det i tillegg eksisterer en egen brukeroversikt med tilknyttede tilganger i informasjonssystemet (for eksempel elektronisk pasientjournal), er det viktig at dataansvarlig sikrer at det til enhver tid er samsvar mellom autorisasjonsregisteret og aktive brukere i informasjonssystemet.

Det skal etableres rutiner for ved behov å kunne sammenstille logger fra hendelsesregistre med autorisasjonsregisteret. Dette kan for eksempel være aktuelt ved innsynsforespørsel fra pasient, for å etterleve kravet om at innholdet skal gjøres forståelig for pasienten.[33]

Det er ikke fastsatt krav i lov eller Normen som angir hvor lenge autorisasjonsregisteret skal oppbevares, men det er fastsatt at den dataansvarlige skal kunne kontrollere hvem som har benyttet seg av tilgangene i ettertid.[34] Oppbevaringstid for autorisasjonsregisteret må derfor vurderes i sammenheng med krav til oppbevaring av logger. Lagringstid for logger omtales i eget faktaark.[35] Ved vurderingen av lagringstid for autorisasjonsregisteret bør virksomheten ta hensyn til at det kan bli nødvendig å kontrollere ansattes tilganger lenge etter at autorisasjonen trekkes tilbake. Det kan derfor være behov for å lagre informasjon om ansattes tilganger etter at ansettelsesforholdet opphører.

## 3.5 Midlertidig tilgang

Midlertidig eller kortvarig tilgang vil typisk gjelde for studenter, vikarer, konsulenter og ved kvalitetssikring av tjenester.

Det skal opprettes avtale med personell som gis midlertidig tilgang, slik at virksomheten har instruksjonsmyndighet og kan gi personellet pålegg om bruk av systemene og taushetsplikt. Det skal opprettes en brukerkonto med tilgang i journalsystemet, og med eget brukernavn og passord eller annen relevant autentisering (se kapittel 4) som samsvarer med behovet for tilgang.

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

## 3.6 Selvautorisering

Selvautorisering gir personell mulighet til å gi seg selv tilgang til helse- og personopplysninger de vanligvis ikke har tjenstlig behov for[36], og på denne måten overstyre de vanlige reglene for tilgang. Selvautorisering er en ordning som kan benyttes der de generelle reglene for tilgangsstyring er til hinder for å yte forsvarlig helsehjelp. Tilgang til funksjoner for selvautorisering skal tildeles personell som en egen rettighet og det bør utarbeides egne rutiner for dette.

Begrepet selvautorisering er et generelt begrep som benyttes i Normen, og ikke et leverandørspesifikt begrep. Leverandører av EPJ-systemer benytter ofte andre begreper som omfatter selvautorisasjon, som for eksempel eksplisitt/begrunnet tilgang eller blålysfunksjon.[37] All tilgang basert på selvautorisasjon skal begrunnes og registreres før opplysningene aksesseres, logges og i etterkant kontrolleres.

I flere etablerte EPJ-systemer er selvautorisering tilgjengelig funksjonalitet i løsningen. Begrunnelsen for selvautorisering skal dokumenteres ved hver bruk. Rent praktisk vil det si at personell må registrere en begrunnelse i journalsystemet for å få åpnet journalen. Dette kan løses ved forhåndsdefinerte begrunnelser eller at personell beskriver begrunnelsen i prosatekst.

[33] Les mer om innsynsretten i kapittel 3.4.1
[34] Pasientjournalforskriften § 13 tredje ledd
[35] Faktaark 15 – Logging og innsyn i logg
[36] Normen 6.0 vedlegg 6.2 Definisjoner
[37] Disse begrepene benyttes i EPJ-systemet DIPS

Et eksempel på behov for selvautorisering er at personell må yte helsehjelp i akuttsituasjoner og må ha tilgang utover den allerede tildelte autorisasjonen. Et annet eksempel er at helsepersonell må finne informasjon om pasienten etter at ytelsen av helsehjelp er avsluttet, på bakgrunn av henvendelse fra pasient eller pasientens fastlege.

***Eksempel:***
Eksempel på roller som typisk gis retten til selvautorisering og får tilgang til ovennevnte funksjonalitet i journalsystemet i en virksomhet, kan være

- leger ved klinisk avdeling på sykehus
- lege eller sykepleier med spesielt fagansvar, f.eks. smertelege/smertesykepleier
- kontorfaglig personell.

Dersom en person bruker selvautorisering for å tilegne seg informasjon vedkommende ikke har rettmessig behov for, regnes det som misbruk av selvautorisering. Misbruk av selvautorisering som avdekkes, for eksempel ved meldinger eller ved kontroll, skal følges opp som et avvik. For å fange opp misbruk skal det for et hvert behandlingsrettet helseregister loggføres hvem som har hentet opp hvilke opplysninger og når, og være mulighet for å rapportere bruk av selvautorisering. Dette kan for eksempel løses med en intern e-post til ansvarlig for oppfølging av bruken eller ved periodiske uttak av og gjennomgang av rapporter over utført selvautorisering.

Hvis det er nødvendig for å ivareta pasientens liv eller unngå alvorlig helseskade, kan selvautorisering brukes også for informasjon som er underlagt reservasjon mot innsyn.

## 3.7 Fjerning eller endring av tilganger

På samme måte som ved tildeling av autorisasjon for tilgang, skal den dataansvarlige eller personalansvarlig leder sørge for at tilganger oppdateres eller deaktiveres ved behov. Endringene skal gjøres innenfor en rimelig tidsramme.

Formålet med å deaktivere tilganger for personer som ikke lengre jobber for virksomheten, eller som bytter stilling eller rolle internt, er å forhindre uautorisert tilgang når personen ikke lengre har tjenstlig behov for tilgang til de aktuelle helse- og personopplysningene.

Behov for fjerning / endring i autorisasjon skjer når

- en medarbeider slutter, slik at tildelt autorisasjon for tilgang skal deaktiveres fra en sluttdato
- en medarbeider begynner i ny stilling i samme virksomhet, slik at eksisterende autorisasjon for tilgang deaktiveres og/eller nye tilganger tilføyes
- et tidsbegrenset engasjement, hospitering eller oppdrag utløper, slik at autorisasjon for tilgang utløper samtidig og helst automatisk
- en medarbeider skal ha permisjon, slik at autorisasjon for tilgang deaktiveres frem til permisjonen er over, med mindre leder beslutter at tilgangene skal opprettholdes i permisjonstiden. Eksempelvis vil det kunne være aktuelt å opprettholde tilgang til e-post og intranett i forbindelse med en permisjon for å holde seg oppdatert på det som skjer i avdelingen under fraværet.

Ved fjerning av autorisasjon for tilgang skal autorisasjonsregisteret oppdateres med dato og klokkeslett for når autorisasjonen for tilgang ble deaktivert.

# 4. Autentisering

Autentisering er i Normen definert som prosessen som gjennomføres for å bekrefte en påstått identitet.[38] Personen som er autorisert for tilgang til opplysninger og informasjonssystemer skal bekrefte sin identitet på en tilstrekkelig sikker måte. Formålet med autentiseringen er altså å sikre at det er den autoriserte personen som gis tilgang til informasjonssystemet eller journalsystemet.

## 4.1 Autentisering i helse- og omsorgssektoren

I helse- og omsorgssektoren har det generelt vært høyere krav til sikker autentisering enn i de fleste andre sektorer, fordi det i så stor grad behandles helse- og personopplysninger.

Journalopplysninger skal bare gjøres tilgjengelig for personell som er tildelt autorisasjon for tilgang og som gjennom autentisering kan bekrefte sin identitet på en sikker måte. Risikovurderingen som skal gjennomføres som beslutningsgrunnlag for tilstrekkelige sikkerhetstiltak for tilgangsstyring, skal også danne grunnlag for valg av sikkerhetsnivå på autentiseringen til informasjonssystemer i virksomheten. Det er viktig at det i risikovurderingen også tas stilling til effektiviteten og enkelheten i prosedyren, i tillegg til grad av beskyttelsesbehov på den informasjonen som gis tilgang til. Kompleksiteten i autentiseringsmekanismene kan ikke være så omfattende at de i praksis kan være til hinder for forsvarlig helsehjelp.

Brukere skal autentiseres med sikker autentiseringsløsning for tilgang til virksomhetens IKT-utstyr og for tilgang til helse- og personopplysninger. Dette gjelder også for tilgang fra mobilt utstyr eller fra hjemmekontor og andre lokasjoner utenfor virksomheten.[39]

Rutiner for autentisering og hvilket sikkerhetsnivå som skal implementeres, bør etableres i styringssystemet for informasjonssikkerhet og personvern før behandling av helse- og personopplysninger starter.

## 4.2 Autentiseringsfaktorer

Autoriserte personer skal tildeles autentiseringsfaktorer[40] for å bekrefte sin identitet før tilgang til opplysninger eller informasjonssystemer gis. Autentiseringsfaktorene skal være unike for hver enkelt for å sikre at kun den autoriserte blir gitt tilgangen det gjelder, i tillegg til at brukeraktiviteter skal kunne spores tilbake til en bestemt person.

Eksempel på autentiseringsfaktorer er

- brukernavn og passord
- brukernavn og passord kombinert med kode som mottas i SMS eller bekreftes gjennom en applikasjon (ulike to-faktor autentiseringsløsninger).
- bruk av elektronisk identitetsbevis (for eksempel BankID, PKI-sertifikat fra Buypass eller Commfides, eller FIDO2-nøkler).

[38] Normen 6.0 vedlegg 6.2 Definisjoner
[39] Normen 6.0 kapittel 5.2.2 Autentisering
[40] I Normen benyttes begrepet «autentiseringskriterier». I veilederen har vi imidlertid valgt å bruke begrepet «autentiseringsfaktorer» da dette også er i tråd med begrepet som benyttes i eIDAS-forordningen.

Tildeling av autentiseringsfaktorer skal gjennomføres på en betryggende måte som ivaretar konfidensialitet og sikrer at kun den autoriserte har kjennskap til sine unike autentiseringsfaktorer.[41] Virksomheten bør etablere pålitelige rutiner for å håndtere tildeling av autentiseringsfaktorer, samt rutiner for hvordan autentiseringsfaktorer på avveie skal håndteres.

***Eksempel på utleveringskrav til autentiseringsfaktorer:***

- Den ansatte møter opp fysisk hos enheten som utsteder ID-/adgangskort og fremviser gyldig legitimasjon.
- Den ansatte blir tilsendt autentiseringsfaktorer i form av en utstedingskode til folkeregistrert adresse. Aktivering av faktoren skjer ved å sende en SMS med koden til utsteders utstedelsessystem. SMSen må sendes fra telefonnummeret som er registrert i personalsystemet.
- Den ansatte blir tilsendt autentiseringsfaktorer til folkeregistrert adresse. Aktivering av faktorene skjer ved elektronisk kontroll av pass og ansiktsgjenkjenning i en app fra utsteder av identifikasjonsmidlet.

Det bør videre utarbeides rutiner for å styre og håndtere autentiseringsfaktorer på virksomhetsnivå for å sikre at disse harmoniserer med helsepersonellets hverdag. Det kan for eksempel være hensiktsmessig å etablere en rutine som sikrer at man ikke bytter passord på fredag ettermiddag, for å unngå at det oppstår utfordringer med brukerkontoene som ikke kan løses før på mandag morgen. Videre bør det tilstrebes å etablere rutiner som gjør pålogging mer brukervennlig og effektiv for helsepersonellet, som for eksempel å ta i bruk «single sign-on» på alle systemer og applikasjoner der dette er mulig. Det er utarbeidet et eget faktaark om bruk og håndtering av passord.[42]

Fellesbrukere i informasjonssystemet eller journalsystemet til virksomheten representerer en risiko, ved at sporbarheten til personell som har utført handlinger blir borte og dermed hindrer ansvarliggjøring og kontroll av tilgang. Fellesbrukere skal derfor ikke benyttes ved tilgang til helse- og personopplysninger. Det kan imidlertid være aktuelt å tillate bruk av fellesbrukere i enkelte situasjoner. Et eksempel er pålogging til felles PCer som ikke gir direkte tilgang til helse- og personopplysninger, fordi pålogging i stedet skjer på enkeltapplikasjoner der opplysningene er lagret. Et annet eksempel et enkelte typer laboratorieutstyr hvor personlig pålogging ikke er hensiktsmessig. I disse tilfellene skal autentiseringsfaktorer besluttes på grunnlag av en risikovurdering.

## 4.3 Sikker autentisering

Styrken på autentiseringsfaktorene er avgjørende for sikkerheten i autentiseringsprosessen. Den totale sikkerheten og styrken på autentiseringen avhenger av antall faktorer som benyttes for å bekrefte identiteten til en person, i tillegg til kompleksiteten til hver enkelt faktor.

Selvdeklarasjonsforskriften[43] definerer tre sikkerhetsnivåer for elektroniske identitetsbevis som gjelder i Norge: «høyt», «betydelig» og «lavt». Disse sikkerhetsnivåene erstatter

[41] Normen 6.0 kapittel 5.2.2 Autentisering
[42] Faktaark 31 Passord og passordhåndtering
[43] Les mer i forskrift om selvdeklarasjon av ordninger for elektronisk identifikasjon

sikkerhetsnivåene 1 til 4 etter «Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor» fra 2008[44], som tidligere gjaldt. De nye sikkerhetsnivåene bygger på det europeiske regelverket, eIDAS-forordningen. Forordningen har som formål å standardisere sikkerhetsnivåer og gi føringer for å oppnå et tilfredsstillende sikkerhetsnivå for elektronisk identifikasjon på tvers av EU/EØS-land.

Tabellen under illustrerer de gjeldende norske sikkerhetsnivåene.[45]

| Sikkerhetsnivå | Beskrivelse av nivået | Utleveringskriterier |
|---|---|---|
| HØYT | Dette sikkerhetsnivået krever to autentiseringsfaktorer, hvorav en er dynamisk.<br><br>Som gyldig identifikasjonsbevis regnes pass eller nasjonal ID-kort. For utenlandsk identitetsbevis må entydig knytning til norsk identitetsnummer godtgjøres. | Aktiveringsprosessen kontrollerer at den elektroniske eIDen ikke er levert til andre enn eIDens eier. Dette innebærer at personens identitet kontrolleres mot personens fysiske kjennetegn, minst en gang. |
| BETYDELIG | Dette sikkerhetsnivået krever to autentiseringsfaktorer, hvorav en er dynamisk.<br><br>Som gyldig identifikasjonsbevis kreves et bevis som representerer den påberoptes identitet og som er godkjent av medlemsstaten. | Etter utstedelse leveres den elektroniske eIDen via en mekanisme som gjør at det kan antas at den bare leveres til eIDens eier, eksempelvis med post til folkeregistrert adresse. |
| LAVT | Dette sikkerhetsnivået krever kun én autentiseringsfaktor.<br><br>Som gyldig identifikasjonsbevis skal kravene for nivå betydelig tilfredsstilles. | Etter utstedelse leveres det den elektroniske eIDen via en mekanisme som gjør at det kan antas at det bare leveres til den tiltenkte personen. |

Vilkårene er kumulative, dvs. at krav til lavere nivåer også må oppfylles på høyere nivåer, med mindre annet eksplisitt fremgår.

Tilbydere av eID-ordninger kan selvdeklarere sine ordninger for eID ved å sende inn en erklæring om at kravene i selvdeklarasjonsforskriften er oppfylt. Dette er en forutsetning for at tilbyderen kan påstå at eID-ordningen er på ett av de tre norske sikkerhetsnivåene.[46] Med andre ord er ikke alle løsninger som krever tofaktorautentisering, automatisk på nivå «betydelig» eller «høyt».

Under følger et eksempel på ulike løsninger innenfor de ulike sikkerhetsnivåene. Eksemplene er i hovedsak hentet fra «Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor».[47]

[44] https://www.regjeringen.no/no/dokumenter/rammeverk-for-autentisering-og-uavviseli/id505958/
[45] Les mer i identifikasjonsnivåforskriften: https://lovdata.no/static/NLX3/32015r1502.pdf
[46] Du kan lese mer om selvdeklarasjon hos Nasjonal kommunikasjonsmyndighet: https://www.nkom.no/internett/elektronisk-id-og-tillitstjenester
[47] Digitaliseringsdirektoratet: https://www.digdir.no/samhandling/veileder-identifikasjon-og-sporbarhet-i-elektronisk-kommunikasjon-med-og-i-offentlig-sektor/2992

***Eksempler på løsninger innenfor de ulike sikkerhetsnivåene:***

*Eksemplene under forutsetter at tilbyder av løsningen har selvdeklarert løsningen hos NKOM.*

**Sikkerhetsnivå lavt**
Dette nivået gir enkel pålogging og tilfredsstiller nivået for mange tjenester. Det gir en viss sikkerhet for at personen er rette vedkommende. Eksempel på løsninger:

- Innlogging med passord som er aktivert ved hjelp av melding til personens e-postadresse i kontaktregisteret eller til folkeregistrert adresse.
- Innlogging med brukerkonto som er aktivert gjennom lenke mottatt i e-post eller SMS til e-postadresse eller telefonnummer registrert i kontaktregisteret.
- Et program (app) på mobil enhet som er knyttet til personen gjennom engangskode sendt til personens mobilnummer i kontaktregisteret.
- Passord, program (app) på mobil enhet eller brukerkonto som er blitt knyttet til personen gjennom innlogging med annen eID i tråd med dette rammeverket.

**Sikkerhetsnivå betydelig**
Dette nivået tilfredsstiller behovet for de fleste tjenester. Eksempel på løsninger:

- MinID, opprettet med engangspassord sendt til folkeregistrert adresse.
- Tofaktorinnlogginger som ikke tilfredsstiller nivå høyt.

**Sikkerhetsnivå høyt**
Dette nivået tilfredsstiller også behovet for tjenester med særlig høye krav til sikkerhet. Eksempel på løsninger:

- eID basert på personlig fremmøte og sentrallagret privatnøkkel.
- eID basert på personlig fremmøte og privatnøkkel lagret på smartkort.

Normen stiller ikke krav til at autentiseringsløsningene som benyttes skal være selvdeklarert for de norske nivåene, men det er krav til at autentisering skal foregå på en sikker måte.[48] Sikre autentiseringsløsninger bør som minimum baseres på tofaktorautentisering hvor brukeren for eksempel autentiserer seg med en kode tilsendt på SMS eller gjennom en app på telefonen, i tillegg til brukernavn og passord. I dette tilfellet er brukernavn og passord én faktor og SMS sendt til et forhåndsregistrert mobilnummer en annen faktor. Den sikreste formen for tofaktorautentisering er autentiseringsløsninger som tilfredsstiller nivå «høyt», som for eksempel bruk av personlige kvalifiserte sertifikater (PKI). Med eIDAS-forordningen åpnes det opp for bruk av andre teknologier enn PKI, som for eksempel biometriske autentiseringsfaktorer og FIDO2 på nivå «høyt». Flere tilbydere av autentiseringsløsninger jobber derfor med å selvdeklarere andre løsninger på nivå «høyt» hos NKOM.

Som nevnt tidligere skal det ligge en risikovurdering til grunn for valg av sikkerhetsnivå på autentiseringen til informasjonssystemer og EPJ i virksomheten. Det kan være hensiktsmessig å beslutte ulike krav til autentiseringsstyrke for innlogging til tjenester med mange følsomme opplysninger kontra tjenester uten følsomme opplysninger, eller til tjenester som er eksponert mot internett kontra tjenester som kun er tilgjengelig på lokalt nettverk.

[48] Normen 6.0, Kapittel 5.2.2 Autentisering

# 5. Kontroll av tilganger

Virksomhetens ledelse skal påse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang.[49] Hovedformålet med kontrollen er å forebygge og avdekke snoking ved å undersøke helsepersonells tilgangsmulighet og faktiske innsyn i pasientopplysninger. Kontrollen vil også være nyttig for å vurdere om helsepersonell har de nødvendige tilgangene for å gi forsvarlig helsehjelp og at tilgangene er i tråd med tjenstlig behov.

Det er ulike kontrolltiltak som vil bidra til å forebygge og avdekke snoking:

- Gjennomgang av tilganger for å kontrollere at tilgangene er i tråd med tjenstlig behov, og sikre at tilganger ajourholdes ved for eksempel bytte av stilling/avdeling eller opphør av arbeidsforhold (se kapittel 5.1).
- Aktivere logging på sentrale funksjoner og etablere en rutine for å aktivt analysere og overvåke loggene (se kapittel 5.2).
- Informasjon til personell med tilgang om at tilganger logges og kontrolleres (personellet har krav på å bli informert).

I tillegg til virksomhetens kontroll, vil også pasientenes rett til innsyn i opplysninger som er registrert på vedkommende, inkludert hvem som har hatt tilgang til opplysningene (se kapittel 6.1), kunne bidra til å forebygge og avdekke snoking. Virksomheten kan imidlertid ikke redusere sin grad av kontroll ved å begrunne det med at pasientene kan bruke innsynsretten.

## 5.1 Gjennomgang av tilganger

Periodisk gjennomgang av tilganger vil være et kontrollerende element som kan bidra til å fange opp avvik fra fastsatte rutiner for tildeling og deaktivering av autorisasjoner. Formålet er å påse at kun de som skal ha autorisasjon for tilgang, faktisk har tilgang, samt påse at nivået på tilgangen er riktig i henhold til vedkommende sine arbeidsoppgaver og er tilrettelagt for å oppfylle tjenstlig behov.

Det er virksomhetens ledelse som skal påse at det jevnlig gjennomføres kontroll av at tilganger er og har vært i tråd med tjenstlig behov.

Gjennomgang og kontroll av tilganger, herunder tildelte autorisasjoner, skal foretas[50]

- ved organisasjonsendringer, overflytting av personell til annen enhet eller endring av arbeidsområde
- minimum årlig (gjerne i forbindelse med sikkerhetsrevisjon)
- ved sikkerhetsbrudd for det informasjonsområdet som blir berørt av bruddet.

Kontrollen bør gjennomføres på et overordnet nivå for ikke å komme i konflikt med taushetsplikten ved at flere enn nødvendig får tilgang til helseopplysninger om pasienten. Med overordnet nivå menes eksempelvis å kontrollere at pasienten er inneliggende eller at

[49] Normen 6.0 kapittel 5.2.3 Kontroll av tilgang
[50] Normen 6.0 kapittel 5.2.3 Kontroll av tilganger

det foreligger en henvisning, istedenfor å gå inn i det enkelte behandlingsforløp for å kontrollere detaljene. Dersom det imidlertid kommer en henvendelse fra pasienten om hvorfor innsynet er gjort, eller ved en eventuell klagesak, skal kontrollen gjøres på detaljnivå for den konkrete saken (se kapittel 6.1).

Dersom kontrollen fører til mistanke om at det har skjedd en urettmessig tilgang, skal virksomhetens ledelse varsles. For øvrig skal hendelsen behandles iht. etablerte rutiner for avviksbehandling, særlig for å få avklart om eksisterende tilgangskontroll er god nok.

## 5.2 Logging av tilgang og brukeraktivitet

Logging skal benyttes som en del av virksomhetens kontroll av tilgangsstyringen. Logging er en muliggjører for å oppdage brudd eller forsøk på brudd på taushetsplikten.

For å oppdage brudd eller forsøk på brudd, er det viktig at loggene analyseres. Det bør gjennomføres en analyse på alle loggoppslag for kombinasjonen loggdata, ansattdata og pasientdata. Analysene bør være risikobaserte. Oppslag som statistisk sett er vanlige (normale) bør antas å være legitime, mens uvanlige oppslag skal vurderes nærmere. Dersom det avdekkes brudd eller forsøk på brudd, skal dette håndteres som avvik[51] og personalmessige reaksjoner vurderes. Dersom personalmessige reaksjoner ikke har nødvendig effekt over tid, det vil si at det er gjentatt tilgang for flere personer som ikke har tjenstlig behov, skal nødvendige tekniske tiltak iverksettes.

Logger skal også benyttes ved innsynsforespørsel fra pasient. Pasientens rett til innsyn er en vel så viktig og effektiv kilde til å avdekke misbruk.[52] Det er derfor viktig at loggene er på et format som kan tolkes av pasienten.

Logging og analyse av logger er også et viktig verktøy for å kartlegge hvorvidt tilgangsstyringen er satt opp på en hensiktsmessig måte som ivaretar både tilstrekkelig sikring av tilgang og begrensing av tilgang. Eksempelvis kan man gjennom analyse av logger få en oversikt over hvor hyppig selvautorisering benyttes, og gjennom dette vurdere om tilgangsstyringen fungerer optimalt. Dersom selvautorisering forekommer hyppig kan det tyde på at tilgangene som er gitt, er for snevre. På den andre siden kan sjelden bruk av selvautorisering signalisere at tilgangene som er gitt, er for vide.

**Hva skal logges?** [53]

I henhold til Normen skal minimum følgende handlinger relevant for tilgangsstyring logges:

- Autorisert bruk av informasjonssystemene
- All system- og administratorbruk til informasjonssystemer og infrastrukturen
- Forsøk på uautorisert bruk av informasjonssystemer og infrastrukturen
- Bruk av selvautorisering.

Med «bruk» menes ikke bare innlogging og bruk av systemer og infrastruktur, men også hvilken type aktivitet brukeren har foretatt seg. Det kan gjelde for eksempel behandling av

[51] Normen 6.0 kapittel 5.4.4 Logging
[52] Les mer om innsynsretten i veilederens kapittel 3.4.1
[53] Normen 6.0 kapittel 5.4.4 Logging

individdata, utdypende vurdering, rettet kontroll, søk etter identitet, eksportering av data, uttrekk fra tabeller og sammenstilling av individdata.

Følgende skal som minimum registreres i loggene ved autorisert bruk av behandlingsrettet helseregister:

- Identiteten til den som har lest, rettet, registrert, endret og/eller slettet helse- og personopplysninger
- Organisatorisk tilhørighet
- Grunnlaget for tilgjengeliggjøringen
- Tidsperioden for tilgjengeliggjøringen.

I tillegg til minimumskravene for hva som skal logges, bør følgende vurderes logget:

- Rollen den autoriserte brukeren har ved tilgangen
- Virksomhetstilhørighet
- Type opplysninger det er gitt tilgang til
- Hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer.

**Analyse av logger**

I Normen er det krav om at elektroniske logger enkelt skal kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd på regelverket.[54]

Ikke alle virksomheter har fått på plass tekniske løsninger og verktøy for å analysere logger, og skal i påvente av dette etablere organisatoriske tiltak på området.[55] Organisatoriske tiltak som kan kompensere for manglende tekniske tiltak, kan for eksempel være å etablere en rutine for jevnlig gjennomgang av logger, der det blir tatt stikkprøver på tilfeldige pasienter. Eksempelet under skisserer hvordan gjennomgangen kan utføres hos en liten virksomhet.

[54] Normen 6.0 kapittel 5.4.4 Logging
[55] Normen 6.0 kapittel 3.4 Risikostyring og risikohåndtering

***Eksempel:***

Normvik Helsesenter er en liten helsevirksomhet som består av åtte behandlende helsepersonell. Normvik Helsesenter har et pågående prosjekt der det jobbes med å få på plass et verktøy for automatisk analyse av logger. I påvente av at prosjektet ferdigstilles har virksomheten, på bakgrunn av en risikovurdering, etablert en rutine for periodisk kontroll av logger som vil kompensere for manglende tekniske tiltak.

Lege Lars har god oversikt over de ansattes tjenstlige behov, og har fått ansvar for å gjennomføre kontrollen av loggene. Hvert kvartal gjennomgår han loggene for å foreta stikkprøver på tilfeldig utvalgte pasienter, for å påse at kravet om tjenstlig behov overholdes. Det hender at kontrollen utføres hyppigere, eksempelvis dersom det er observert avvik i tidligere gjennomganger eller ved pasientinnsyn, eller dersom annen informasjon indikerer at kontrollen bør utføres. Hvor mange stikkprøver som utføres hvert kvartal har også en risikobasert tilnærming, og avhenger blant annet av antall pasienter og behandlinger for inneværende periode. I tillegg til den tilfeldige utvelgelsen av pasienter, foretas det også stikkprøver på pasienter som er særlig utsatt for snoking, som for eksempel kjente personer og tidligere ansatte.

Når kontrollen er gjennomført, registreres dette i internkontrollsystemet. Avvik som eventuelt oppdages rapporteres til daglig leder, som har ansvar for avvikshåndtering og vil vurdere personalmessige reaksjoner.

For å etablere tilstrekkelige tiltak for å oppdage uautoriserte handlinger og sikkerhetstruende hendelser, bør det brukes en kombinasjon av tekniske tiltak og manuelle rutiner for analyse av logger. Ved fastsettelse av metode for å analysere logger bør det gjøres en totalvurdering av hva som er tilstrekkelig i hvert enkelt tilfelle.

For ytterligere detaljer om hvordan logging kan benyttes for å avdekke uautorisert bruk eller forsøk på uautorisert bruk av helse- og personopplysninger, samt detaljer om hvordan logger skal sikres og oppbevares, henvises det til dokumentet Logging og innsyn i logg (faktaark 15).[56]

[56] Faktaark 15 Logging og innsyn i logg

# 6. Rettigheter

## 6.1 Pasientens rettigheter

### 6.1.1 Pasientens rett til innsyn

Pasientens innsynsrett er en viktig del av kontrollen av tilgangsstyring, og bidrar til å hindre misbruk av tilgangsrettigheter og sikre etterlevelse av prinsippet for tjenstlig behov. En pasient har rett til innsyn i opplysninger registrert om seg selv i behandlingsrettet helseregister og fagsystem. Innsynet gjelder også loggen over hvem, og fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger og på hvilket tidspunkt.[57]

Enhver virksomhet som behandler helse- og personopplysninger, er pliktig til å tilrettelegge for at den registrerte får innsyn i opplysningene på forespørsel. Det bør utarbeides egne rutiner for å sikre at den registrertes rettigheter til innsyn blir ivaretatt, samt rutiner for å vurdere påstander fra pasienter om mistenkt misbruk.

Les mer om retten til innsyn i eget veiledningsmateriell.[58]

### 6.1.2 Pasientens reservasjonsrett

En pasient har rett til å motsette seg helsepersonells tilgang til sine helseopplysninger, samt rett til å nekte informasjonsutveksling mellom helsepersonell, selv om opplysningene er nødvendige for å yte helsehjelp. Kun dersom tungtveiende grunner taler for det kan utlevering likevel skje.[59] Det kan for eksempel være dersom det er fare for liv eller alvorlig helseskade.

Når en pasient benytter seg av reservasjonsretten, skal helsepersonellet nedtegne kravet fra pasienten i journalen. Det skal i journalsystemet kunne håndteres og være funksjonalitet som tilrettelegger for sperringen for hele eller deler av journalen ved tilgang eller utlevering. Journalen skal kunne sperres for enkeltpersonell, en gruppe av helsepersonell eller virksomheter. Reservasjonsretten skal også ivaretas ved tilgang mellom virksomheter.

Ønsker pasienten å gjøre unntak fra sperringen, skal det 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 eller ikke gjelder en bestemt situasjon eller behandling.

Flere nasjonale e-helsetjenester har lovhjemmel for å behandle og lagre helse- og personopplysninger digitalt, uten at pasienten må samtykke på forhånd. Dette gjelder for eksempel Kjernejournal og Kommunalt pasient- og brukerregister (KPR). For disse løsningene har pasienten iht. lovverket rett til å reservere seg mot en slik behandling og lagring. Virksomheter som forvalter tjenestene, må ha en løsning for å administrere og håndheve slike reservasjoner.

---

[57] Normen 6.0 kapittel 4.2.3 Innsyn
[58] Veileder for rettigheter ved behandling av helse- og personopplysninger kapittel 4 og Faktaark 15 om logging og innsyn i logg
[59] Helsepersonelloven §§ 25 og 45, samt pasient- og brukerrettighetsloven § 5-3

## 6.2 Medarbeideres rettigheter

Logger regnes som personopplysninger. All bruk av loggene, inkludert innsamling, oppbevaring og bruk i oppfølging av det enkelte helsepersonell, må oppfylle kravene i personopplysningsloven. Virksomheten som er dataansvarlig må blant annet sikre at den oppfyller informasjonsplikten, kravet til lovlighet og de øvrige personvernprinsippene i personvernforordningen artikkel 5.[60] Dersom loggene skal brukes i kontrolltiltak overfor ansatte bør virksomheten være oppmerksom på arbeidsmiljølovens krav til saklig grunn, proporsjonalitet, forutgående informasjon, drøfting med tillitsvalgte og evaluering.[61] Les mer om rettslige rammer for bruk av logger i kontrolltiltak overfor ansatte okumentet Logging og innsyn i logg (faktaark 15).

[60] Les mer om dette i faktaark 57 om personvernprinsippene, https://www.ehelse.no/normen/faktaark/faktaaark-57-personvernprinsippene

[61] Se arbeidsmiljøloven kapittel 9 og Arbeidstilsynet og Datatilsynets veileder om kontroll og overvåking i arbeidslivet

Endringshistorikk

| Dato | Versjon | Endring |
|---|---|---|
| 17.03.22 | 2.0 | Revidert iht. Normen 6.0. |
| | | |
| | | |
| | | |

# Vedlegg

## A. Definisjoner

For forklaring på generelle ord og uttrykk benyttet i denne veilederen henvises det til vedlegg «6.2 Definisjoner» i Normen 6.0. Det er i midlertidig enkelte ord og uttrykk som er spesifikke for denne veilederen og dermed ikke er definert Normen 6.0. Definisjonen av disse følger i listen under.

- S -

Med «**single sign-on**» menes en autentiseringsprosess som lar brukeren få tilgang til flere applikasjoner ved kun å logge inn én gang, for eksempel at det å logge på PCen/det lokale nettverket gir direkte tilgang til å åpne en applikasjon uten å i tillegg måtte logge inn i applikasjonen.

- T -

Med «**tofaktorautentisering**» menes en autentiseringsprosess som krever to ulike faktorer ved innlogging til informasjonssystemene.

# B. Enkel sjekkliste for tilgangsstyringsprosessen

Under følger en sjekkliste som kortfattet oppsummerer anbefalinger til tilgangsstyringsprosessen.

### Tilrettelegging og forberedelser

- ☐ Det er definert og implementert en tilgangsstruktur som ivaretar taushetsplikten og prinsippet om tjenstlig behov. Tilgangsstrukturen er basert på en risikovurdering.
- ☐ Det er etablert rutiner som ivaretar kravene til tilgangsstyring, herunder autorisering, autentisering og kontroll av tilganger.
- ☐ Det er definert hvilke personer/stillinger i virksomheten som har myndighet til å tildele autorisasjon og bestille brukertilganger.
- ☐ Det er definert hvilke personer/stillinger i virksomheten som har tilgang til å opprette brukere og tilganger i hvert enkelt informasjonssystem.

### Opprettelse av brukertilganger

- ☐ Det er etablert en rutine for opprettelse og tildeling av brukertilganger i informasjonssystemene. Rutinen kan enten omfatte manuelle eller automatiserte prosesser, og skal ivareta følgende punkter:
  - ☐ Det gjennomføres en identitetskontroll av brukeren. Korrekt identitet registreres i et master-register dersom dette ikke er foretatt på et tidligere stadium.
  - ☐ Bestilling av bruker og tilganger skal følge etablerte rutiner. Det skal kunne spores hvem som har godkjent bestillingen.
  - ☐ Brukeren opprettes med standardtilganger (og ved behov også med tidsbegrensning) i tråd med sin funksjon, dersom annet ikke er spesifisert i bestillingen.
  - ☐ Autorisasjonsregisteret oppdateres i tråd med tildelingen av tilgangen.

### Endring og vedlikehold av brukertilganger

- ☐ Det er etablert en rutine for endring og vedlikehold av brukertilganger i informasjonssystemene. Rutinen kan enten omfatte manuelle eller automatiserte prosesser, og skal ivareta følgende punkter:
  - ☐ Gamle tilganger deaktiveres ved bytte av stilling, endring i arbeidsoppgaver eller bytte av lokasjon.
  - ☐ Nye tilganger opprettes i tråd med ny stillingsbeskrivelse, nye arbeidsoppgaver eller ny lokasjon.
  - ☐ Det gjennomføres kontroll av tilganger og autorisasjoner jevnlig for å påse at disse er i tråd med tjenstlig behov.

**Deaktivering av brukertilganger**

- Det er etablert en rutine for deaktivering av brukertilganger i informasjonssystemene. Rutinen kan enten omfatte manuelle eller automatiserte prosesser, og skal ivareta følgende punkter:
  - Det meldes ifra til de som jobber med brukeradministrasjon, som for eksempel systemeiere eller IT-personell, når en ansatt har sagt opp.
  - Ansatte som slutter får tilgangene sine deaktivert i alle informasjonssystem og infrastruktur ved sluttdato.
  - Ansatte som slutter leverer inn utlevert utstyr på sluttdato, som for eksempel PC, adgangskort og autentiseringsfaktorer.
  - Det gjennomføres kontroll av aktive brukere opp mot ansatte som har sluttet, for å påse at alle tilganger deaktiveres.