VEILEDNING OG SELVDEKLARERING FOR DELOMRÅDE:

Kravnumrene nedenfor refererer til Faktaark 38 - Sikkerhetskrav for systemer

Autori-sering Kravnr. 1 til 18	Autentisering Kravnr. 19 til 24	Hendelses-registrering Kravnr. 25 - 31	Pasientrettigheter Kravnr. 32 til 35	Integritet Kravnr. 36 til 37

1 INFORMASJON OM SELSKAP

Tabellen nedenfor bør fylles ut av leverandøren med informasjon om virksomheten og objektet.

Leverandørnavn:		
Postadresse:		
Besøksadresse:		
Organisasjonsnummer:		
Kontaktinformasjon:	***Navn på kontaktperson:***	
	E-post:	***Telefonnummer:***
Objekt:	***Benevnelse på system:***	***Hovedversjon:***
	Benevnelse delsystem:[1]	***Versjon:***
	Kommentar for å utdype beskrivelsen av objekt:	
Utfylt:	***Dato:***	***Utfylt av person:*** ☐ Samme som kontaktperson

1. *Selvdeklareringen kan være avgrenset til et bestemt delsystem. Om selvdeklareringen gjelder hele systemet med alle sine eventuelle delsystemer skal ikke hvert enkelt delsystem beskrives. I slike tilfeller angis kun systemet med en eventuelt utdypende kommentar. Eksempler på delsystem kan være: en modul i systemet, en integrasjon som hører inn under systemet og som leveres med systemet.*

2 SELVDEKLARERING AV AUTORISERING

Med autorisering menes at en person, i et ansettelsesforhold, i en bestemt rolle gis en bestemt rettighet til: lesing av tekst og bilder, registrering, redigering, retting, sletting og/eller sperring av helse- og personopplysninger. Autorisasjonen skal registreres i et autorisasjonsregister.

Krav Nr. 1	Kravet i Normens kapittel **5.2** er: *Tilgangsstyring skal etableres for alle behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer*
Hensikt med kravet	Tilgangsstyring skal sørge for at tilgang til behandlingsrettede helseregistre og fagsystem kun gis ut fra tjenstlig behov
Veiledende beskrivelse	Dette kravet er selvdeklarert når alle obligatoriske krav vedrørende autorisering er selvdeklarert. Tilgangsstyring betyr at det skal være funksjonalitet som gjør at: - den enkelte bruker innehar (er autorisert i) en rolle - den enkelte bruker må tildeles rettighet for tilgang til helse- og personopplysninger (autorisering) - rettigheten er knyttet til en eller flere roller - rettigheten tilpasses det tjenstlige behovet for tilgang brukeren har Tilgangstyringen skal kunne tilpasses ut fra det tjenstlige behovet. Elementer i dette er autorisering, autentisering og ytelsen til Den registerte. Tilgangsstyringen skal kunne tilpasses behovet i den enkelte virksomhet og virksomhetens organisering. Tilgangsstyringen skal ikke kunne slås av. Begrunnelsen for dette er at tilgangstyring er et lovkrav.
Veiledende eksempel	I eksemplet nedenfor vises funksjoner som kan etableres i systemet for å oppfylle kravet til tilgangsstyring: - Opprette og endre virksomhet - Opprette og endre organisatoriske enheter i virksomheten - Opprette og endre formål med tilhørende rettigheter - Opprette og endre roller med tilhørende rettigheter - Opprette og endre bruker - Knytte bruker til rolle med rettigheter iht formålet med tilgang - Opprette og endre ansettelsesforhold bruker har i virksomhet - Opprette og endre beslutning om tilgang til helse- og personopplysninger - Legge til en oppføring i autorisasjonsregisteret - Lagre en oppføring i autorisasjonsregister i 5 år - Opprette og endre autentiseringskriteria (for eksempel passord) - Knytte autentiseringskriterium til bruker og rolle - Autorisering hvor bruker må autentisere seg i rett rolle med rett autentiseringskriteria - Muligheter til å konfigurere autentisering hvor bruker må autentisere seg i ny rolle ved rollebytte - Hendelsesregistrere all tilgang til helse- og personopplysninger - Lagre oppføring i hendelsesregister så lenge det er bruk for dem

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 2	Kravet i Normens kapittel **5.2.1**er: *Autorisering skal skje selvstendig for hver enkelt rolle*
Hensikt med kravet	Ved autorisering av en bruker skal autoriseringen gjøres for en konkret rolle som brukeren har tjenstlig behov for.
Veiledende beskrivelse	Funksjonen for autoriseringing skal være slik at brukeren kan autoriseres for den enkelte rollen. Den enkelte autorisering skal medføre en egen oppføring i autorisasjonsregisteret, om det fins i systemet, hvor formålet med autorisasjonen (for eksempel yte helsehjelp, administrasjon av helsehjelp, forskning, kvalitetssikring) registreres. Jf krav nr 4.
Veiledende eksempel	I et system der den enkelte bruker autoriseres til kun en rolle og alltid vil forbli i den ene rollen, kan systemet ha funksjonalitet slik at brukeren automatisk blir tildelt denne rollen og ikke må aktivt velge roller hver gang brukeren logger seg på systemet.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:

Krav Nr. 3	Kravet i Normens kapittel **5.2.1**er: *Ulike ansettelsesforhold skal identifiseres*
Hensikt med kravet	I tilfeller hvor samme person har tilgang til helse- og personopplysninger i en virksomhet og opptrer med flere ansettelsesforhold, skal autorisasjon gis for det enkelte ansettelsesforhold.
Veiledende beskrivelse	Med begrepet ansettelsesforhold, i kravet, menes både fast ansatte, vikarer og ulike personer som har et oppdrag for eksempel gjennom en tilbyder av helsepersonell. For å oppfylle kravet må systemet ha funksjonalitet for å knytte en bruker til en eller flere ansettelser.
Veiledende eksempel	For eksempel kan det samme helsepersonellet jobbe 3 dager i uken som tilsatt i en virksomhet og 2 dager i uken som innleid helsepersonell fra en annen virksomhet. I dette eksempelet skal brukeren ha 2 ansettelser knyttet til seg og autoriseringen skal være for selvstendig for den enkelte ansettelse. Det vil si at det i dette tilfellet skal det opprettes en bruker per virksomhet. For eksempel kan identifisering av ulike ansettelsesforhold løses ved at personen tildeles to ulike brukeridentiteter.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:

Krav Nr. 4	Kravet i Normens kapittel **5.5.2** er: *All tildeling av autorisasjon skal registreres i et autorisasjonsregister*
Hensikt med kravet	Autorisasjonsregisteret kan være en del av systemet og autorisasjonsregisteret skal da vise utstedte autorisasjoner.
Veiledende beskrivelse	Velger leverandøren å inkludere autorisasjonsregisteret i systemet er det kravene nedenfor som skal selvdeklareres. Det er ikke et krav at autorisasjonsregisteret skal føres elektronisk. Normalt i en virksomhet vil autorisasjonsregisteret være summen av autorisasjoner gitt i ulike systemer. Autorisasjonsregisteret kan føres manuelt, i et system som har et autorisasjonsregister eller at autorisasjonsregisteret er summen av registreringer i flere systemer. Et elektronisk autorisasjonsregister kan likevel være i et system der autorisasjoner som er gitt i andre systemer blir ført. Det må finnes en funksjon som automatisk registrerer en oppføring i autorisasjonsregisteret ved tildeling av autorisasjon til en bruker. Det registreres en ny oppføring i autorisasjonsregisteret: - for hver ny rolle brukeren autoriseres for - når autorisasjonen endres
Veiledende eksempel	

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 5	Kravet i Normens kapittel **5.2.2** er: *Databehandlingsansvarlig skal sørge for at det opprettes et autorisasjonsregister. Registeret skal som minimum inneholde:* - *informasjon om hvem som er tildelt autorisasjon* - *til hvilken rolle autorisasjonen er tildelt* - *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)* *Utdypning av kravet: Det skal også registreres hvem (fysisk identifiserbar person) som har opprettet (registrert) autorisasjonen*
Hensikt med kravet	Autorisasjonsregisteret skal vise hvem som er og var tildelt hvilke roller og rettigheter og hvem som har tildelt og registrert autorisasjonen. Registeret skal på en enkel måte gi databehandlingsansvarlig informasjon om hvilke brukere som har og hadde hvilke roller med tilhørende rettigheter.
Veiledende beskrivelse	Velger leverandøren å inkludere autorisasjonsregisteret i systemet er det kravene nedenfor som skal selvdeklareres. Med begrepet ”databehandlingsansvarlig” må dette leses slik at systemet har støtte for at den databehandlingsansvarlige kan ivareta kravet. Autorisasjonsregisteret kan være summen av autorisasjoner gitt i ulike systemer. Autorisasjonsregisteret kan føres manuelt, i et system som har et autorisasjonsregister. Følgende dataelementer skal minimum skal registreres: - entydig identifikator for brukeren som er tildelt autorisasjon (f.eks. en bruker-ID) - navnet på brukeren som er tildelt autorisasjon - virksomhet (navnet på virksomheten brukeren tilhører) - organisatorisk enhet (navnet på den organisatoriske enhet brukeren tilhører) - hvilken rolle autorisasjonen er tildelt (Det må også registreres hvilke rettigheter rollen gir, ettersom rettighetene for rollen kan endres etter at rollen er tildelt brukeren) - formålet med autorisasjonen (for eksempel yte helsehjelp, administrasjon av helsehjelp, forskning, kvalitetssikring) - tidspunkt for når autorisasjonen ble gitt (dato og klokkeslett) - tidspunkt for når autorisasjonen var/er gyldig fra (dato og klokkeslett) - tidspunkt for når autorisasjonen eventuelt ble endret (dato og klokkeslett) - tidspunkt for når endringen var gyldig fra (dato og klokkeslett). - tidspunkt for når autorisasjonen eventuelt ble tilbakekalt (for eksempel ved fratredelse eller permisjon) (dato og klokkeslett) - entydig identifikator til den som har registrert autorisasjonen - navnet til den som har registrert autorisasjonen - entydig identifikator til den som har tildelt eller endret autorisasjonen. Her menes den ansvarlige leder som har godkjent at brukeren tildeles autorisasjonen - navnet til den som har tildelt eller endret autorisasjonen. Her menes den ansvarlige leder som har godkjent at brukeren tildeles autorisasjonen
Veiledende eksempel	

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐
Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:			

Krav Nr. 6	Kravet i Normens kapittel **5.2.2** er: *Ved tilgang til helseopplysninger mellom virksomheter skal autorisasjonen tidsbegrenses*
Hensikt med kravet	Ivareta kravet om at tilgang til helseopplysninger i annen virksomhet skal tidsbegrenses innenfor det som er avtalt mellom virksomhetene.
Veiledende beskrivelse	Kravet gjelder enhver tilgang til helseopplysninger i andre virksomheter. Om det aktuelle systemet ivaretar initiering, oppkobling, autentisering, overføring mv. av helseopplysinger må systemet kunne tidsavgrense autorisasjonen for helsepersonellet. Tidsbegrensningen bør gjelde for: - År - Måned - Dag - Klokkeslett Om systemet ikke gir tilgang til andre virksomheters gjelder ikke kravet for det aktuelle systemet.
Veiledende eksempel	

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:

Krav Nr. 7	Kravet i Normens kapittel **3.3.4** er: *5 års lagring minimum fra det tidspunkt dokumentet ble tatt ut av bruk:* - *Oversikt over tildelte autorisasjoner og tilganger til helse- og personopplysninger (autorisasjonsregister)*
Hensikt med kravet	Hensikten er at databehandlingsansvarlig i ettertid, for kontrollformål, skal vite hvilken autorisasjon med tilhørende rolle brukeren hadde på et angitt tidspunkt.
Veiledende beskrivelse	Med begrepet "*dokumentet*" i kravet menes i denne sammenhengen den enkelte oppføring i autorisasjonsregisteret (record). Autorisasjonsregisteret kan være summen av autorisasjoner gitt i ulike systemer. Autorisasjonsregisteret kan føres manuelt, i et system som har et autorisasjonsregister. Velger leverandøren å inkludere autorisasjonsregisteret i systemet er det kravene nedenfor som skal selvdeklareres. Med kravet menes at den enkelte oppføring i autorisasjonsregisteret skal oppbevares (arkiveres) i minimum 5 år fra det tidspunktet (dato og klokkeslett) autorisasjonen ble trukket tilbake (tatt ut av bruk). Det må finnes en funksjon som automatisk oppdaterer autorisasjonen i autorisasjonsregisteret fra det tidspunkt autorisasjonen trekkes tilbake. Med trekkes tilbake menes at - Autorisasjonen utløper på dato (hvis autorisasjonen er tidsbegrenset) - Leder avslutter (stenger) brukerens autorisasjon På det tidspunkt autorisasjonen trekkes tilbake må følgende dataelement i autorisasjonsregisteret oppdateres: - tidspunkt for når autorisasjonen eventuelt ble tilbakekalt (for eksempel ved fratredelse eller permisjon) (dato og klokkeslett)
Veiledende eksempel	For å gi databehandlingsansvarlig fleksibilitet kan systemet gi mulighet til å sette en lengre lagringstid enn 5 år. Dette kan gjøres ved å angi antall år (ett år er lik 365 dager) oppføringen i autorisasjonsregisteret skal lagres. Antall år kan uansett ikke være mindre enn 5 år. For å slette oppføringer i autorisasjonsregisteret som overstiger lagringstiden (minimum 5 år) kan det for eksempel være en funksjon som automatisk løper gjennom alle oppføringer i autorisasjonsregisteret og sletter oppføringer som overstiger minimum lagringstid. Videre bør rollen brukeren er autorisert til arkiveres sammen med oppføringen i autorisasjonsregisteret. Rollen må lagres med alle tilhørende rettigheter. Med dette menes for eksempel hvilke menyvalg, skjermbilder, funksjoner, dokumenter, osv som har vært tilgjengelig for rollen. Videre hvilke oppgaver rollen har hatt rettigheter til. For eksempel lese (inklusive utskrift), registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 8	Kravet i Normens kapittel **5.2.2** er: *Tildelt autorisasjon skal sikre at den enkelte kan få tilgang til relevante og nødvendige helse- og personopplysninger i samsvar med personellets ansvar og oppgaver* *Utdypning av kravet: Tildelt autorisasjon skal kunne tidsavgrenses*
Hensikt med kravet	Med begrepet "*den enkelte*", i kravet, menes i denne sammenhengen personellet (brukeren). Med kravet menes at når brukeren autoriseres skal det gis tilgang til helse - og personopplysninger som samsvarer med det tjenstlige behovet.
Veiledende beskrivelse	Systemet må ha funksjonalitet som sikrer at rettighetene som tildeles en rolle er tilpasset brukerens ansvar og oppgaver. Med relevante menes at opplysningene må være relevante for den oppgaven som den autoriserte har. Med tilpasset menes at det må være mulig å definere rettighetene i den enkelte rolle slik at de samsvarer med ansvar og oppgaver (tjenstlig behov). Utdypning av kravet sier at systemet også skal ha funksjonalitet for å tidsavgrense autorisasjonen. Det betyr at det må være funksjonalitet for å registrere en stoppdato for den tildelte autorisasjonen. Systemet skal automatisk stoppe autorisasjonen fra og med den registrerte stoppdatoen.
Veiledende eksempel	Hver rolle skal settes opp slik at brukerens tjenstlige behov for tilgang blir ivaretatt gjennom de rettighetene som hører til rollen. Med dette menes at det skal velges for eksempel hvilke menyvalg, skjermbilder, funksjoner, dokumenter, osv som skal være tilgjengelig for rollen. Videre skal det velges hvilke oppgaver rollen skal ha tilgang til. For eksempel lese (inklusive utskrift), registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 9	Kravet i Normens kapittel **5.2.2** er: *For personer som har ulike roller i virksomheten, skal autorisering skje for hver rolle uavhengig av vedkommendes øvrige roller*
Hensikt med kravet	Hensikten med kravet er at bruker skal benytte ulike roller ift tjenstlige behov og hvilke oppgaver som skal utføres.
Veiledende beskrivelse	Med begrepet "*roller i virksomheten*" i kravet menes i denne sammenhengen rolle i systemet som skal selvdeklareres. Det må finnes funksjonalitet for at den enkelte bruker kan tildeles autorisasjon for flere uavhengige roller. Det etableres en funksjon i skjermbilde for autorisering av bruker hvor det er mulig å knytte flere roller til den enkelte bruker. En tildelt rolle skal ikke kunne endres slik at en enkelt bruker får utvidede eller begrensede tilganger ift de tilganger rollen i utgangspunktet gir. Alle endringer av en rolle skal gjelde for samtlige som er autorisert i rollen.
Veiledende eksempel	Helsepersonelloven § 48 angir eksempler på roller som kan benyttes i systemet. Utvalget av roller og spesifikasjon av tilhørende rettigheter kan avhenge av virksomhetens størrelse og organisering. Om det er et rolleregister kan rolleregisteret inneholde predefinerte roller som er relevante for den delsektoren systemet er beregnet for. Virksomheten bør kunne opprette og konfigurere egne roller som er relevante for sin virksomhet. Kravet kan for eksempel ivaretas ved bruk av to ulike bruker-ID der brukeren plasseres i en rolle ved pålogging. Bruker må da bytte bruker-ID ved normal av/pålogging for å benytte den andre rollen.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 10	Kravet i Normens kapittel **5.2.2** er: *Autorisasjon for å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger skal gis til dem som har tjenstlig behov*
Hensikt med kravet	Med kravet menes at det ved tildeling av autorisasjon skal skilles på hvilke rettigheter den enkelte bruker skal ha, ut fra sitt tjenstlige behov for tilgang til helse- og personopplysninger.
Veiledende beskrivelse	Ved autorisering av brukeren skal det være funksjonalitet for å angi hvilket formål brukeren skal ha med sine rettigheter. Formålet skal registreres i autorisasjonsregisteret, om autorisasjonsregisteret inngår i systemet. Deretter skal rollen med tilhørende rettigheter som passer med formålet velges.
Veiledende eksempel	Eksempler på rettigheter: - lese; brukeren kan se informasjon om Den registrerte og helseopplysninger (skjerm, utskrift) - registrere; brukeren kan opprette nye Den registrerte og tilhørende helseopplysninger - redigere; brukeren kan endre opplysninger om Den registrerte og helseopplysninger - rette; brukeren kan endre helseopplysninger. Retting skal skje ved at helseopplysninger føres på nytt, eller ved at en datert rettelse tilføyes i helseopplysningene. Retting skal ikke skje ved at opplysninger eller utsagn slettes. (jf. helseregisterloven 42, http://lovdata.no/all/tl-19990702-064-008.html#42) - slette; brukeren kan fjerne opplysninger om Den registrerte og helseopplysninger - sperre; brukeren kan sperre helseopplysninger. (jf helseregisterloven § 28, http://lovdata.no/all/hl-20010518-024.html#28) Rettighetene kan også kombineres og gis det detaljeringsnivået som er nødvendig for det enkelte system.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 11	Kravet i Normens kapittel **5.2.2** er: *Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for større mengder helse- og personopplysninger*
Hensikt med kravet	Med kravet menes at teknisk personell (IT-personell) med utgangspunkt i tjenstlig behov kan autoriseres for tilgang til hele eller deler av helse- og personopplysningene i systemet. Begrunnelsen er at IT-personell har behov for tilgang for å kunne bistå brukere i ulike situasjoner. Løsninger hvor teknisk personell benytter administratorrettigheter til databaser eller filsystemer dekkes ikke av beskrivelsen.
Veiledende beskrivelse	Begrepet "*teknisk personell*" i kravet forstås vidt kan for eksempel omfatte administrator av systemet, superbruker og brukerstøtte. Begrepet "*større mengder*" i kravet må tolkes ut fra det enkelte system og bruksområdet. Det bør gjennomfores en forholdsmessighetsvurdering for systemet som skal selvdeklareres. En forutsetning for beskrivelsen nedenfor er at teknisk personell autoriseres i systemet og benytter ordinær autentiseringsløsning som omtalt i andre krav. Systemet må ha funksjonalitet som gjør at enkelte roller kan tildeles rettigheter som gir tilgang til "større mengder" opplysninger. Hvilke muligheter som skal finnes for å angi "større mengder" vil være avhengig av type system og hvilken delsektor systemet benyttes i. Det kan være behov for at rettighetene skal kunne begrenses til enkeltavdelinger eller virksomhet, slik at rollen som tildeles konfigureres etter behov. Kravet til dokumentasjon av en konkret beslutning for tilgang gjelder også for teknisk personell.
Veiledende eksempel	Kravet gjelder som eksplisitt nevnt kun teknisk personell. En bruker av systemet kan for eksempel autoriseres for tilgang til store mengder helse- og personopplysinger ifm. utsendelse av SMS eller utarbeidelse av dagplaner.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐
Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":			

Krav Nr. 12	Kravet i Normens kapittel **5.2.3** er: *Tilgang til behandlingsrettede helseregistre skal gis etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for medisinsk behandling av pasienten*
Hensikt med kravet	Kravet betyr at tilgang skal styres slik at taushetspliktreglene ivaretas og at tilgang til helse- og personopplysninger ikke gis til andre enn de som har tjenstlig behov. Med tjenstlig behov menes at brukeren skal ha tilgang tilpasset ansvar og oppgaver.
Veiledende beskrivelse	Kravet medfører at det registreres en beslutning for å få tilgang til helse- og personopplysninger. Registreringen kan utføres av en bruker eller den kan være systemgenerert. Når beslutningen er avsluttet skal tilgangen stenges på den måten at bruker må angi beslutning på nytt for å få tilgang. Når bruker avslutter sin tilgang skal det angis beslutning på nytt for å få tilgang.
Veiledende eksempel	Løsningen kan bygges slik at bruker velger beslutning fra et beslutningsregister eller registrerer beslutning i et tekstfelt. Nedenfor er det gitt noen eksempler på beslutninger: • Den registrerte henvender seg til helsepersonellet per telefon eller ved fremmøte • Den registrerte ønsker å fornye en resept • Den registrerte bestiller time for konsultasjon og tar i den sammenheng opp egen helsetilstand som skal registreres • Den registrerte kommer til avtalt time • Den registrerte ytes helsehjelp • Resultat av blodprøve skal registreres i laboratoriesystem • Resultat av blodprøve skal vurderes av lege • Den registrerte har trukket seg som blodgiver • Helsepersonellet skal tolke bilder for diagnostikk • Vurdere søknad om kommunal tjeneste Virksomheten bør kunne opprette og redigere egne beslutninger om tilgang som er relevante for sin virksomhet. Systemet kan ha funksjonalitet for å gi korrekt beslutning på forhånd før tilgangen benyttes. Eksempel kan være at den registrerte har bestilt eller blitt innkalt til time og systemet automatisk gir korrekt beslutning når brukeren autentiserer seg i systemet.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 13	Kravet i Normens kapittel **5.5.2** er: *Systemet som administrerer autorisasjon skal skille mellom rettigheter til å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger*
Hensikt med kravet	Hensikten med kravet er at systemet skal ha funksjonalitet for å administrere tilgang og rettigheter ift det tjenstlige behovet brukeren skal ha.
Veiledende beskrivelse	Systemet må ha funksjonalitet for å knytte de enkelte rettighetene for å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger til roller.
Veiledende eksempel	Rettighetene kan for eksempel være så detaljerte at databehandlingsansvarlig kan regulere rettighetene til det enkelte dokument (informasjonselement i systemet) eller deler av et dokument som inneholder helse- og personopplysninger.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 14	Kravet i Normens kapittel **5.2.6 og 5.5.2** er: *Hendelsesregistrene, autorisasjonsregister og tilstedeværelsesregister skal sikres mot endring og sletting av uautorisert personell.* *Hendelsesregistrene skal sikres mot endring og sletting av uautorisert personell*
Hensikt med kravet	Hendelsesregistrene, autorisasjonsregister og tilstedeværelsesregister er kontrollregistre som skal benyttes ved konstatert eller mistanke om sikkerhetsbrudd. Registrene skal av den grunn ikke kunne endres eller slettes av brukeren som har benyttet systemet.
Veiledende beskrivelse	Systemet bør ha funksjonalitet for å opprette en rolle med rettigheter til å endre og slette hendelsesregistrene, autorisasjonsregister og eventuelt tilstedeværelsesregister. Med endring menes å endre innholdet i hele registeret eller i enkeltoppføringer ved hjelp av funksjonalitet i skjermbilder, scripts eller en form for redigeringsverktøy (editor). Med sletting menes at alle eller deler av oppføringene i registeret slettes permanent.
Veiledende eksempel	Med tilstedeværelsesregister menes et register som viser faktisk tilstedeværelse av personell, for eksempel hendelsesregister fra adgangskontroll (nøkkelkort), timeregistreringssystem og stemplingsur. Tilstedeværelsesregisteret kan også inneholde informasjon om bruk av mobilt utstyr og hjemmekontor.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for ”Ja”, ”Nei”, ”Ikke relevant”:

Krav Nr. 15	Kravet i Normens kapittel **5.5.2** er: *Dersom det er åpnet for nødrettstilgang, skal tekniske tiltak etableres på en slik måte at helsepersonell i nødrettssituasjoner, kan få tilgang til nødvendige helse- og personopplysninger. Slik tilgang skal grunngis og registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ))*
Hensikt med kravet	Hensikten med å grunngi og registrere bruk av nødrettstilgang er å hindre at bruker benytter nødrettstilgang som generell løsning for tilgang til helse- og personopplysninger.
Veiledende beskrivelse	Forutsetningen for denne beskrivelsen er at leverandøren har valgt å etablere løsning for nødrettstilgang i systemet. Begrunnelse for den enkelte bruk av nødrettstilgang skal dokumenteres og registreres i systemet. Hva som ligger i begrepet "*nødvendige helse- og personopplysninger*", i kravet, må vurderes ut fra det enkelte system. Kravet gir i prinsippet ikke noen begrensninger i omfanget av tilgangen til helse- og personopplysninger.
Veiledende eksempel	Løsningen for å begrunne bruk av nødrettstilgang kan baseres på at bruker registrerer begrunnelse i et fritekstfelt eller at bruker velger fra en forhåndsdefinert liste med begrunnelser.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 16	Kravet i Normens kapittel **4.4.2** er: *Nødrettstilgang kan etableres som en mulighet for autoriserte brukere til å gi seg selv tilgang uten å følge fastsatte prinsipper for å få tilgang til helse- og personopplysninger*
Hensikt med kravet	Nødrettstilgang skal sikre tilgang til helse- og personopplysninger hvor de ordinære prinsippene for tilgangsstyring ikke kan følges. For å avverge fare eller skade kan det være behov for øyeblikkelig tilgang til helse- og personopplysninger, og det ut fra de foreliggende omstendigheter må vurderes som rettmessig.
Veiledende beskrivelse	Forutsetningen for denne beskrivelsen er at leverandøren har valgt å etablere løsning for nødrettstilgang i systemet. Systemet må ha funksjonalitet for å autorisere en bruker til bruk av nødrettstilgang. Hva som ligger i begrepet "*nødvendige helse- og personopplysninger*" i kravet, må vurderes ut fra det enkelte system. Kravet gir i prinsippet ikke noen begrensninger i omfanget av tilgangen til helse- og personopplysninger.
Veiledende eksempel	

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 17	Kravet i Normens kapittel **4.4.2** er: *Begrunnelsen for nødrettstilgang skal dokumenteres og hvert enkelt tilfelle skal følges opp som et avvik.*
Hensikt med kravet	Hensikten med å følge opp hvert enkelt tilfelle med bruk av nødrettstilgang som avvik, er å kontrollere at nødrettstilgang kun benyttes for å avverge fare eller skade.
Veiledende beskrivelse	Forutsetningen for denne beskrivelsen er at leverandøren har valgt å etablere løsning for nødrettstilgang i systemet. Systemet skal ha funksjonalitet til å autorisere bruker i en rolle for å kunne søke i hendelsesregistre etter bruk av nødrettstilgang. Jf. Krav Nr 28.
Veiledende eksempel	Det kan være en funksjon for rapportering om bruk av nødrettstilgang i systemet.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐

Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":

Krav Nr. 18	Kravet i Normens kapittel **6.5** er: *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* *Ved tilgang til helseopplysninger mellom virksomheter skal det i tillegg kontrolleres hvorfor tilgangen er benyttet og tidsperioden helseopplysningene er hentet fram.* *Utdypning av kravet: Behandlingsrettet helseregister inkl elektronisk pasientjournal (EPJ) eller fagsystem må ha funksjonalitet slik at kontrollen kan gjennomføres effektivt.*
Hensikt med kravet	Hensikten med kravet er at virksomhetens ledelse ved behov skal kunne kontrollere hvem som har hatt tilgang til helseopplysninger.
Veiledende beskrivelse	Med begrepet "*Virksomhetens ledelse*" i kravet, menes i denne sammenhengen at systemet har funksjonalitet slik at virksomhetens (kundens) ledelse kan ivareta kravet. Systemet må ha funksjonalitet for å autorisere bruker i en rolle som gir tilgang til kontrollfunksjonen. Kontrollfunksjonen skal ha en søkefunksjon for å hente frem brukere i definerte roller. I tillegg skal den registrerte kunne søkes frem. Ved tilgang til helseopplysninger som er gitt til andre virksomheter må søkefunksjonen kunne hente fram data om hvorfor tilgangen er benyttet og tidsperioden helseopplysningene er hentet fram.
Veiledende eksempel	Funksjonen for å gjennomføre søket kan for eksempel være i en rolle eller del av en rolle. Ett eksempel på en slik rolle kan være supervisor (superbruker). Resultatet av søket kan for eksempel gi informasjon om: Brukeren - Søkekriteriene (bruker, rolle, Den registrerte, tidsavgrensning) - Entydig identifikator for brukeren - Rollen den autoriserte brukeren hadde ved tilgangen - Formålet med den tildelte autorisasjonen (registrert i autorisasjonsregisteret) Den registrerte - Den registrertes identitet (for eksempel fødselsnummer / d-nummer og navn) - Tidspunkt (dato og klokkeslett) og varighet for bruk av tilgangen. - Om tilgangen gjelder en annen virksomhet bør søket innholde tidsperiode og beskrivelse av hvorfor tilgangen ble benyttet - Hvilke type helseopplysninger det er gitt tilgang til - Beslutningen for tilgang (registrert for den enkelte tilgang) Rapporten bør kunne tas ut på skjerm og papir. Det bør finnes funksjon for å tidsavgrense (dato/klokkeslett fra og dato/klokkeslett til) et søk. Kontrollen kan gjøres slik at det verifiseres at tjenstlig behov for tilgangen er i samsvar med: - formålet med den tildelte autorisasjonen - beslutningen for tilgang For eksempel kan rolle og formål være det samme.

Selvdeklarerer leverandøren kravet?	Ja ☐	Nei ☐	Ikke relevant ☐
Kort redegjørelse og/eller henvisning til leverandørens dokumentasjon for "Ja", "Nei", "Ikke relevant":			