Mottaker etter liste

20.09.2019

Innspill til ny versjon av Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, versjon 6.0

Vedlagt er utkast til versjon 6.0 av Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, heretter kalt Normen.

Normen er en bransjenorm som er utarbeidet og forvaltes av organisasjoner og virksomheter i sektoren. Normen skal bidra til tilfredsstillende informasjonssikkerhet og godt personvern hos den enkelte virksomhet og i sektoren generelt. Den skal bidra til at det etableres mekanismer hvor virksomhetene kan ha gjensidig tillit til at øvrige virksomheters behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Utkastet sendes på bred og åpen høring. Vi ønsker innspill både fra virksomheter og ansatte i helse- og omsorgstjenesten, fra leverandører og databehandlere, fagorganisasjoner, små helsevirksomheter, private helsevirksomheter, de registrerte (pasienter, brukere, ansatte, innbyggere mv.) og alle andre som berøres av Normens krav.

Frist for innspill: 1. november 2019.

Overordnet om innholdet i versjon 6.0

Med bakgrunn i ny lovgivning, teknologisk utvikling og store enkelthendelser med mye oppmerksomhet har det i de senere år vært et økt fokus på personvern og informasjonssikkerhet i helse- og omsorgssektoren. Som en følge av dette har man også fått et økt behov for oppdatert veiledning og en modernisert og oppdatert Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.

Denne versjonen av Normen er resultatet av et langvarig revisjons- og utviklingsarbeid. Hovedmålene har vært å sikre at Normens krav er dekkende for nye krav i personvernforordningen og samtidig tilpasset nåtidens teknologi. Det har også vært et viktig mål å forenkle fremstillingene og gjøre Normen mer leser- og brukervennlig.

Det er gjort flere endringer fra forrige versjon. Det er blant annet tatt inn nye krav, tekst er slettet og krav er presisert eller endret. Normens virkeområde er endret og kravet til forholdsmessighet kommer tydeligere frem. Det er gjort en gjennomgang og forenkling av teksten, samtidig som noe tekst er tatt ut og flyttet til veiledningsmateriellet.

Spesielt om forenkling og økt leser- og brukervennlighet

Det er gjort et betydelig arbeid med å øke leser- og brukervennligheten. Flere krav er endret, noen krav er slettet, noen krav er nye.

En stor del av forenklingsarbeidet ligger også i tydeliggjøring av hvilke krav som gjelder for hvilke virksomheter og ved hvilke behandlinger. Dette er bl.a. gjort gjennom å være konsekvente på bruken av "skal"- og "bør"-krav

Normen har fått en total språklig gjennomgang.

Spesielt om små virksomheter

Små virksomheter som legekontor, tannlegekontor, fysioterapeuter og psykologpraksiser, kjennetegnes av at de har enkle og oversiktlige IT-løsninger og ofte få ansatte. De har selv ansvar for informasjonssikkerhet, IT- sikkerhet og IT oppgavene internt. I motsetning til et stort helseforetak med ressurser og kompetanse, har de små virksomhetene i liten grad ressurser og kunnskap om informasjonssikkerhet og personvern.

Virksomheten skal uansett størrelse, sørge for å ha tilfredsstillende informasjonssikkerhet. Dette innebærer at virksomheten etablerer rutiner for internkontroll som ivaretar informasjonssikkerheten og personvernet på en tilstrekkelig måte. Rutinene skal dokumenteres.

Normen v6.0 er bedre tilpasset små virksomheters arbeid gjennom forenkling, presisering og økt leser- og brukervennlighet.

Parallelt med arbeidet med ny versjon av Normen blir det også utarbeidet en ny veileder for små virksomheter. Formålet med veiledningsmateriellet er å bidra til tydeligere og mer tjenestetilpassede krav for de små virksomhetene i helse og omsorgssektoren

Spesielt om sekundærbruk[1]

Det er presisert at Normen gjelder sekundærbruk så langt kravene passer. Flere av kravene i Normen er endret slik at de også skal kunne passe sekundærbruk. Det er også lagt til enkelte krav for sekundærbruk.

Overordnet om endringer i kapittel 1

Det er gjort endringer i kapittel 1.4 Virkeområde – hva Normen regulerer. Endringen klargjør at Normens virkeområde omfatter både dataansvarlig og databehandler, helse- og omsorgstjenesten og leverandører, både de som behandler personopplysninger og de som ikke gjør det.

Normen gjelder for alle som ved avtale er forpliktet til å følge Normen, se kap. 1.3. Det er i dag flere som forpliktes ved avtale til å følge Normen som ikke omfattes av v5.3s tekst i kapittel 1.4 Virkeområde-hva Normen regulerer. Endringen gjøres for at det ikke skal oppstå misforståelser om hvem som faktisk forpliktes til å følge kravene.

Der er også gjort endringer i samme kapittel som omhandler sekundærbruk.

Kapittel 1.2 EUs personvernforordning (GDPR) er slettet. Noe av innholdet er flyttet til andre steder i Normen og noe er slettet.

---

[1] Behandling av helseopplysninger til statistikk, helseanalyser, forskning, kvalitetsforbedring, planlegging, styring og beredskap i helse- og omsorgsforvaltningen og helse- og omsorgstjenesten.

Det er gjort enkelte endringer i kapittel 1.2 Formål.

Overordnet om endringer i kapittel 2

Sentralt for endringer i kapittel 2 er en betraktelig forenkling og "slanking" av tekst som enten var veiledende eller gjengivelse av personvernforordningen. En god del av denne teksten flyttes til faktaark. Det er gjort endringer i delkapittel om roller og ansvar, innarbeidet personvernprinsippene etter artikkel 5 i personvernforordningen, samt en tydeliggjøring at Normen også gjelder databehandlere ved å ha et eget delkapittel i kapittel 2 om databehandleres ansvar.

Overordnet om endringer i kapittel 3

Også i kapittel 3 er en gjort betraktelig forenkling og "slanking" av tekst som enten var veiledende eller tatt fra personvernforordningen. En god del av denne teksten flyttes til faktaark. Det er innarbeidet et nytt delkapittel om forholdsmessighet ved valg av tiltak (3.1) og minimumskravene for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet i kapittel 3.2 er endret. Disse endringene er i stor grad en forenkling og tydeliggjøring av minimumskravene. I tillegg er kapittel 3. 5 om personvernkonsekvensvurdering forenklet og tydeliggjort at virksomheter skal gjennomføre en overordnet vurdering før en fullskala DPIA skal gjennomføres.

Overordnet om endringer i kapittel 4

Kapittelet er omstrukturert og inneholder flere nye krav. Tema for kapittelet er behandlingsgrunnlag og krav og plikter til virksomhetenes behandling av helse- og personopplysninger. Flere av virksomhetenes plikter er direkte utledet av pasientrettigheter eller personvernrettigheter. Pasient og bruker har mange rettigheter etter helselovgivningen. Fokuset for Normen er noen av de pasientrettighetene som også er personvernrettigheter eller som direkte gjelder personvern og informasjonssikkerhet.

Normen 6.0 er oppdatert etter ny pasientjournalforskrift, og opphevingen av forskrift om tilgang mellom virksomheter. Retting, sletting og sperring er nå generelt omtalt.

Det er utdypet hvordan dataansvarlig skal sørge for kontroll og oversikt over tilgang til sine helseopplysninger fra andre virksomheter.

Overordnet om endringer i kapittel 5

Kravene om leverandørforhold og avtaler er blitt klarere med tanke på hvilke krav i Normen som er relevante ut fra type leveranse og tjeneste som ytes. Virksomhetenes ansvar for leverandøroppfølging i alle faser av en leverandørrelasjon er utdypet i tråd med anbefalingene i Direktoratet for e-helse sin rapport fra 2017 om informasjonssikkerhet ved bruk av private leverandører. Skytjenester er nå omtalt i Normen.

For å ivareta endringer i trusselbildet rettet mot virksomheter i sektoren er begrepet sikkerhetsarkitektur introdusert og nye krav til informasjonssikkerhet innarbeidet. Kravene er harmonisert med NSMs grunnprinsipper for IKT-sikkerhet.

Økonomiske og administrative konsekvenser

Det er gjort en betydelig jobb for å forenkle krav og språk og presisere hvilke krav som gjelder for hvem. Flere krav er tatt ut. Denne forenklingen bør ha en positiv økonomisk konsekvens for flere virksomheter.

Normens krav bidrar til å sikre virksomhetenes informasjon og verdier. Nye krav og tilhørende tiltak er dels utnyttelse av eksisterende sikkerhetsfunksjonalitet i operativsystem og fagsystem og nye rutiner. For enkelte virksomheter krever det investering i tekniske sikkerhetsløsninger.

Tydeliggjøring av kravene bør medføre større presisjon i hvilke krav som stilles ved leveranser til sektoren, og dermed en forenkling. Krav som er nye i versjon 6.0 kan medføre at virksomheten og virksomhetens ledelse må vie noe mer oppmerksomhet til informasjonssikkerhet og personvern, men dette bør for de fleste virksomhetene i sektoren allerede være i tråd med etablert praksis f.eks. ved innføringen av EU personvernforordning.

Endringen av virkeområde, se over, er en presisering av dagens praksis og bør dermed ikke ha store økonomiske og administrative konsekvenser.

Utkast til nytt vedlegg – Oversikt over Normens krav med bl.a. tilhørende hjemmelsoversikt, tidligere Faktaark 6b og 38

I versjon 6.0 av Normen er faktaark 6b og 38 innarbeidet som et vedlegg. Faktaarket er omstrukturert og utvidet og inneholder nå oversikt over hvilke lovhjemler kravet eventuelt bygger på. Dette vedlegget vil også inneholde en oversikt over Normens krav sammenstilt med ISO 27001, annex A.

Utkastet viser konseptet og tar utgangspunkt i Normen versjon 5.3.

Konkrete områder vi ønsker innsikt i

Vi ønsker innspill på hele utkastet. Og i tillegg noen konkrete områder vi ønsker mer innsikt i. Spørsmålene peker på noen av hovedmålsetningene med revisjonen av Normen.

1. Er Normens virkeområde nå dekkende for det Normen bør dekke?
2. Er Normens virkeområde nå tydelig nok? Vil f.eks. en leverandør forstå om virksomheten er forpliktet til å følge Normens krav?
3. I nytt kapittel 4 er det gjort et utvalg av temaer og behandlingsaktiviteter.
   a) Gir kapittelet verdi for brukerne?
   b) Er det noen viktig som mangler?
4. Et av hovedmålene har vært å øke leser- og brukervennlighet. Dette er gjort gjennom forenkling av tekst, fjerning av krav, språklig gjennomgang, profesjonsnøytralitet og generell språkvask. Vi ønsker tilbakemeldinger på dette.
5. Ved å gjennomgående bruke "skal" og "bør" samt peke på forholdsmessighet og "egnede" tiltak både i kap 1.4 og 3.1 forsøker Normen v6.0 å vise at virksomheten selv må vurdere og ta valg om hva som er egnede tiltak. Kommer dette tydelig nok frem? Er det f.eks. tydelig hvilke informasjonssikkerhetskrav som gjelder sekundærbruk og er det lettere for en liten virksomhet og forstå hvilke krav som gjelder for den?

Innspill og videre prosess

Utkastet til versjon 6.0 er jobbet fram av referansegrupper med representanter fra sektoren, diskusjoner i styringsgruppen for Normen, innspill innkommet gjennom arbeidet med versjon 5.3, løpende innspill til sekretariatet for Normen og diskusjoner i sekretariatet.

Endringer i dokumentet er markert ved at tekst som er ny eller endret er markert i blått. Endringer i eksisterende tekst er gjort blå der innholdet i kravet er endret eller der de tekstlige endringene er vesentlige.

Innspill på utkastet gis på vedlagte mal og sendes til sikkerhetsnormen@ehelse.no

Versjon 6.0 legges frem til godkjenning for Normens styringsgruppe 3. februar 2020.

Vi oppfordrer virksomhetene som blir gjort kjent med denne høringen å bidra til å sikre at alle brukere av Normen, f.eks. også små virksomheter og helsepersonell, deltar.

Virksomhetene som er representert i styringsgruppa for Normen vil også få informasjon om høringen og utkastet til Normen v6.0 tilsendt sin representant.

Innspillsmøter

Det vil bli avholdt to innspillssmøter hos Direktoratet for e-helse på Skøyen 23. september. Der vil vi gå gjennom de viktigste endringene, og ta imot og diskutere innspill.

- Åpent innspillsmøte kl 10-12. Åpent for alle interesserte. Vi oppfordrer pasient- og brukerorganisasjoner å komme. Dette vil også bli streamet.
- Leverandørmøte kl 13-15. Åpent for leverandører og databehandlere, med spesielt fokus på disse. Dette vil ikke bli streamet.

Mer informasjon og lenke til streaming kommer på www.normen.no

Atferdsnorm etter art. 40 i Personvernforordningen

Samtidig som Normen v6.0 godkjennes av styringsgruppen for Normen, vil styringsgruppen ta stilling til om Normen v6.0 skal oversendes til Datatilsynet for formell godkjenning som en adferdsnorm etter reglene i personvernforordningen.

Ved spørsmål kontakt sekretariatet for Normen.

- E-post: sikkerhetsnormen@ehelse.no
- Jan Gunnar Broch, leder for sekretariatet for Normen, tlf. 90179293
- Aasta Margrethe Hetland, prosjektleder, tlf. 90089189

Med hilsen,

Jan Gunnar Broch

Leder av Normens sekretariat

(Elektronisk godkjent)

Vedlegg:

- Høringsutkast Normen v6.0
- Innspillsmal Normen v6.0
- Utkast_vedlegg_Oversikt over Normens krav
- Mottakere av høringen