



Datatilsynet

# Strategi for godt personvern i helsesektoren

Juni 2011



## Sentrale personvernprinsipper

Noen prinsipper står sentralt i oppbyggingen av personvernlovgivningen. Prinsippene bygger på et grunnleggende ideal om at den enkelte skal ha bestemmelsesrett over personopplysninger om seg selv.

### **Saklig begrunnelse**

Behandling av personopplysninger skal være saklig begrunnet. Opplysningene skal kun samles inn til uttrykkelig angitte og legitime formål, og brukes i overensstemmelse med disse.

### **Frivillig samtykke**

Registrering av personopplysninger skal i størst mulig grad være basert på et frivillig, uttrykkelig og informert samtykke. Opplysninger i offentlige registre hvor registrering er pliktig, skal være lovhjemlet.

### **Opplysningsplikt for den behandlingsansvarlige**

Ved innhenting av personopplysninger har den enkelte rett til å få vite om det er frivillig eller obligatorisk å oppgi personopplysningene, hvilket formål opplysningene skal brukes til, og om de vil bli utlevert til andre.

### **Rett til innsyn**

Den registrerte har rett til innsyn i opplysninger som gjelder en selv. Den ansvarlige skal bistå den registrerte med å gi innsyn i hvilke opplysninger som er lagret, hva de skal brukes til, og hvor de er hentet fra.

### **Registreringen skal være riktig**

Opplysningene som registreres skal være korrekte og oppdaterte.

### **Feilaktige opplysninger skal rettes**

Feilaktige personopplysninger skal rettes eller slettes.

### **Unødvendige opplysninger skal slettes**

Overskuddsinformasjon og opplysninger som ikke lenger er nødvendige for formålet med registreringen, skal slettes.

### **Informasjonssikkerhet skal ivaretas**

Den behandlingsansvarlige skal sørge for tilfredsstillende informasjonssikkerhet. Det må kunne dokumenteres at rutiner og tiltak som sikrer personopplysningene blir etterlevd i praksis. Risikovurderingene må ta hensyn til at brukerne har ulike forutsetninger for å ivareta egen informasjonssikkerhet.

### **Strengere regler ved følsomme opplysninger**

Behandling av følsomme personopplysninger er underlagt særlig strenge regler.

## Innholdsfortegnelse

Sentrale personvernprinsipper.....	2
Hva er personvern? .....	4
Personvern i helsesektoren.....	5
Sentrale helseregistre.....	6
Kvalitetsregistre.....	8
Helseforskning.....	10
Lokale behandlingsrettede helseregistre .....	12
Tilgangsstyring i journalsystem .....	15
Tilgang på tvers av helseforetak og kjernejournal .....	17
Ny teknologi i helsevesen og omsorgssektoren .....	20
Vedlegg I: Begrepsavklaringer .....	23
Vedlegg II: Tankemodell - registerform.....	24
Vedlegg III – Prinsipper for innebygd personvern (privacy by design).....	25

## Hva er personvern?

Helsesektoren er en storforbruker av sensitive personopplysninger. Sektoren har derfor høy prioritet i Datatilsynets arbeid. Tilsynet er opptatt av at personvernets kår balanseres mot andre hensyn på en tilfredsstillende måte. Det danner samtidig bakgrunn for dette dokument, hvor tilsynet trekker opp mulige tilnærminger til de utfordringene som er identifisert. Innledningsvis vil tilsynet imidlertid trekke opp en del viktige prinsipper innenfor personvernet, som gjelder på tvers av de ulike samfunnssektorer. Deretter vil tilsynet spisse de generelle prinsippene i forhold til helsesektoren.

Sentralt i personvernet står det enkelte menneskets ukrenkelighet og krav på respekt fra andre mennesker, respekt for egen integritet og privatlivets fred. Personvernet er derfor nært knyttet til enkeltindividers mulighet for privatliv, selvbestemmelse og selvutfoldelse. Retten til privatliv følger blant annet av den europeiske menneskerettskonvensjon (EMK) artikkel 8 og står sentralt i EUs personverndirektiv (95/46 EF).

Et vesentlig element i personvernet er at personer i utgangspunktet skal kunne bestemme hva andre skal få vite om hans eller hennes personlige forhold. Vi kan i denne sammenhengen snakke om "personopplysningsvern", og det er primært denne dimensjonen som er underlagt omfattende lovregulering som for eksempel personopplysningsloven, helseregisterloven, regler om taushetsplikt.

Selvbestemmelsesretten er imidlertid ikke uinnskrenket. Hensynet til samfunnets interesser kan veie tyngre enn hensynet til den enkelte. Personvernidealet tilsier imidlertid at det i størst mulig grad skal være et godt utviklet tillitsforhold mellom registrerte personer og den som behandler opplysninger om dem. Folk skal med andre ord i minst mulig grad ha grunn til å føle usikkerhet og frykt når personopplysninger blir behandlet uavhengig av hva de registrerte har samtykket til, eller om behandling av personopplysninger er hjemlet i lov. Det finnes likevel en nedre grense for hvor lite selvbestemmelse den enkelte kan sitte igjen med uten at dette kommer i konflikt med grunnleggende menneskerettigheter.

Personvernidealet og personvernlovgivningen er ikke avgrenset til spørsmål om den enkeltes rett til å bestemme hvem som kan få tilgang til opplysningene, men innebærer også krav til hvordan personopplysninger skal behandles. Særlig er krav til opplysningenes kvalitet, retten til innsyn i egne personopplysninger og sikring av personopplysninger viktig. Ivaretagning av personvern handler derfor også om at det stilles krav til kvalitet i personopplysninger og til infrastrukturer og informasjonssystemer der slike opplysninger finnes, og ikke bare om retten til å begrense eller sette vilkår for tilgang til personopplysninger. Manglende informasjons- og systemkvalitet vil kunne gi en rekke uønskede konsekvenser og skade så vel ideelle som økonomiske interesser, både for enkeltindivider, organisasjoner og for samfunnslivet generelt.

## Personvern i helsesektoren

Helsesektoren involverer i praksis samtlige innbyggere på ulike stadier i livet. Opplysningene som behandles i sektoren er blant de mest beskyttelsesverdige både etter tilsynets vurdering og enkeltpersonens oppfatning. Samtidig må en gi fra seg svært mange opplysninger i "bytte" mot helsehjelp. Den enkelte har begrenset kontroll med spredningen av disse opplysningene.

Tillit mellom pasient og behandlende helsepersonell er en forutsetning for å yte helsehjelp av god kvalitet. Dersom pasienten ikke stoler på behandleren, vil han kunne holde tilbake viktig informasjon. Resultatet kan bli manglende eller feilaktig behandling. Personvern i relasjon til helsesektoren dreier seg om pasientens autonomi, forsvarlig håndtering av helseopplysninger og at korrekte opplysninger tilflyter riktige behandlere.

Datatilsynet er i denne strategien opptatt av å balansere personvern mot andre viktige samfunnshensyn.

Sektoren er preget av høy grad av endringsvilje og evne – fra departement til institusjonsnivå. Dette binder Datatilsynet ytterligere til en vesentlig tilstedeværelse i sektoren. Særlig aktuelt nå er samhandlingsreformen og modernisering av helseregisterområdet.

Det ligger klare føringer om at Datatilsynet ivaretar en aktiv kontrollvirksomhet etter helseregisterloven og helseforskningsloven.

Datatilsynets mål er at

- nye løsninger og nytt regelverk i sektoren skal ivareta personvernet på en bedre måte, spesielt med hensyn til registerform og individets selvbestemmelse
- tilgangsstyring og logging i sektoren skal styrkes, og sektoren skal påvirkes til å bidra mer positivt til dette
- individets mulighet til å ha oversikt og kontroll med opplysninger om seg selv skal styrkes, og det skal legges bedre til rette for at individet kan benytte sine rettigheter

At alle parter har en balansert forståelse for disse tre grunnleggende behovene er nødvendig for at samfunnet får en god helsetjeneste med godt personvern. Datatilsynet ønsker å bidra til dette.

## Sentrale helseregistre

*Norge ble rangert lavt på personvernbeskyttelsesnivå av Privacy International i 2007. Dette skyldtes blant annet at Norge har relativt mange helseregistre og at det er mulig å koble disse med hverandre. Dagens sentrale helseregistre er alle etablert uten samtykke eller reservasjonsadgang, og de fleste med identitetshåndteringen internt. Obligatorisk registrering av identitet i et sentralt helseregister innebærer en utfordring for personvernet. Nasjonalt helseregisterprosjekt har dessuten foreslått at det etableres 11 nye fellesregistre.*

### Utfordringer

Intensjonene med helseregistrene er gode. Kunnskap om pasientene er nyttig for å utvikle og kvalitetssikre helsetjenesten. Fellesregistermodellen<sup>1</sup> som nå er under utvikling, er komplisert og det er utfordrende å se hvilke personvernmessige konsekvenser denne kan medføre fullt ut. Dette gjør det krevende å formidle personvern hensyn og skape forståelse for personvernets betydning i helsevesenet og i befolkningen. Datatilsynet har også inntrykk av at bevisstheten i befolkningen er lav knyttet til hvor uthullet taushetsplikten er blitt og i hvor stor grad helseopplysningene faktisk spres og registreres til ulike formål.

Behovet for kunnskap og hensynet til den enkeltes personvern må balanseres. I denne forbindelse vil den enkeltes rett til selv å få velge sentral registrering være et sentralt moment. Det er også viktig at identitetshåndteringen skjer på en måte som er best forenlig med et godt personvern.

Sentrale helseregistre inneholder sensitiv informasjon om en stor del av Norges befolkning. Med et slikt volum er det krevende å innhente samtykke fra de registrerte. Ingen av de sentrale helseregistrene er i dag samtykkebaserte. En utfordring for personvernet er hvordan selvbestemmelsesretten best kan ivaretas. Der hvor samtykke ikke er mulig, er det nødvendig å se på reservasjonsløsninger som et kompensierende tiltak.

En reservasjonsløsning vil føre med seg en ny utfordring, nemlig hvordan pasienten skal informeres om at han blir registrert og hvilke rettigheter han har til å reservere seg.

Flere sentrale registre ønskes opprettet i forholdsvis nær fremtid, og det vil være viktig å få godt personvern bygget inn i registrene allerede fra starten. Det er et godt personvernprinsipp at registrene skiller mellom pasientens identitet og helseopplysninger, og at disse oppbevares ulike steder. Det må dessuten være et mål at personvern fremmende teknologi benyttes i så stor grad som mulig.

### Aktørene:

- **Helse og omsorgsdepartementet** har det overordnede ansvaret for at befolkningen får gode helse- og omsorgstjenester og styrer disse gjennom et omfattende lovverk og årlige bevilgninger.
- **Helsedirektoratet** iverksetter viktige deler av politikken på helseområdet.
- **Folkehelseinstituttet (FHI)** både bruker og forvalter de fleste sentrale helseregistrene. I tillegg er de sekretariat for Nasjonalt helseregisterprosjekt og en betydelig aktør når det gjelder etablering av helseregistre.

---

<sup>1</sup> Nærmere beskrevet i vedlegg I.

- **Interesseorganisasjonene** for brukerne og profesjonsutøverne er viktige aktører som ofte har fokus på personvern i sin politikkutforming.

## Datatilsynets posisjon

Følgende prinsipper legges til grunn:

- Det er viktig å finne en god balanse mellom hvordan kunnskapsbehov og pasientenes personvern skal ivaretas.
- Helseregistret skal ikke identifisere pasienten i større grad enn det som er nødvendig for å oppfylle formålet med registret.
- Helseopplysninger og identitetsopplysninger skal oppbevares atskilt.
- Det gir best personvern dersom identitetsopplysningene oppbevares eksternt. Da minimeres risikoen med tanke på snoking, følgene av helseopplysninger på avveier reduseres betraktelig og tilliten til at personvernet er ivaretatt øker.
- Det bør stilles spørsmål ved om formålet med flere helseregistre kunne vært oppfylt selv om registret ble pseudonymisert.
- Sentrale helseregistre kan kun opprettes uten samtykke i den grad det er nødvendig for å oppnå formålet med registret. De mest inngripende og sensitive helseregistrene bør baseres på samtykke fra pasienten.
- Borgerne må som hovedregel ha adgang til å reservere seg mot registrering i helseregistre, og reservasjonsadgangen må sikres gjennom god informasjon og en enkel og lett tilgjengelig reservasjonsløsning.

## Datatilsynets strategi

Datatilsynet skal

- bidra til en balansert tilnærming til kunnskapsbehov og pasientens personvern - dette avhenger blant annet av registerform, obligatorisk eller valgfri registrering, inngrepets størrelse og formålet med registret, se vedlegg II
- arbeide for at flest mulig sentrale helseregistre får en uttrykkelig reservasjonsrett
- være tydelig på at helseregistre med de aller mest sensitive helseopplysningene må være samtykkebaserte (for eksempel sentralt register over psykiske lidelser og rusmisbruk og sentralt legemiddelregister)
- jobbe for løsninger som sikrer at helseopplysninger og identitet oppbevares atskilt og at identitetshåndteringen i størst mulig grad skjer eksternt
- bidra til samarbeid med Helse- og omsorgsdepartementet, Helsedirektoratet og FHI for å få inn gode personvernløsninger tidlig i prosessen med utvikling av nye helseregistre

## Kvalitetsregistre

*Med kvalitetsregistre menes helseregistre som er opprettet for å drive kvalitetssikringsarbeid på lokalt, regionalt eller nasjonalt nivå. Feltet skiller seg fra forskning som drives for å skaffe ny viten. Med innføringen av helseforskningsloven tydeliggjøres det hva som er kvalitetsregistre på lokalt nivå. Lokale kvalitetsregistre kan som utgangspunkt opprettes uten konsesjon fra Datatilsynet.*

## Utfordringer

### Om lokale kvalitetsregistre

Innføringen av helseforskningsloven har tvunget frem en avklaring om hvilke registre som faller utenfor forskningsbegrepet og følgelig innefor kvalitetssikringsbegrepet. Dette er helseopplysninger som behandles på siden av journal for å følge opp kvaliteten i helsehjelpen.

Datatilsynet har over tid observert en viss sammenblanding mellom forskningsregistre og kvalitetsregistre, og at det er behov for en gjennomgang av praksis i sektoren. Første steg ble tatt ved innføringen av helseforskningsloven.

Det er trolig at det fremdeles er utfordringer knyttet til det rettslige grunnlaget for en rekke registre med formål som ikke klart faller innefor rammene for forskningsregistre eller lokale kvalitetssikringsregistre. Slike vil trenge konsesjon fra Datatilsynet. Lokale kvalitetsregistre kan opprettes med hjemmel i helsepersonellovens § 26. Det er her begrensninger med hensyn til formål, omfang og varighet før det inntreer en konsesjonsplikt. Videre er det krav om begrensning av identifiseringsgrad, medbestemmelse i den grad det er hensiktsmessig, og at opprettelsen av registeret skal være ledelsesforankret.

### Om regionale og nasjonale kvalitetsregistre

Regionale og nasjonale kvalitetsregistre er normalt konsesjonsbelagte, og de er som hovedregel basert på samtykke. Innføringen av fellesregistermodellen, først ved hjerte- og karregisteret, vil gi hjemmel i lov for enkelte av disse registrene. Dette medfører en endring i hvordan Datatilsynet følger opp disse registrene.

Det fremstår videre som en utfordring at det etableres lokale kvalitetsregistre for å rapportere til de regionale / nasjonale registrene. Disse driftes i flere tilfeller av samme part som drifter det nasjonale registeret.

## Aktørene:

- **Helse- og omsorgsdepartementet (HOD) og Helsedirektoratet (HD)** er sentrale i klargjøring av krav i sektoren, og for lovgivning og iverksettelse av politikk på området. Disse aktørene vil også bli sentrale i utvikling av regelverket ved innføringen av fellesregistermodellen.
- **Helseforetakene (HF)** er den størst aktørgruppen når det gjelder kvalitetsregistrene.

- **Senter for klinisk dokumentasjon og evaluering (SKDE)** ved UNN har fremstått som en sentral aktør for regionale og nasjonale registre. De driver blant annet nettstedet [www.helseregister.no](http://www.helseregister.no)
- **Fagmiljøer i regionene** er sentrale sammen med **Nasjonalt folkehelseinstitutt (FHI)** og **Nasjonalt kunnskapssenteret for helsetjenesten** som nasjonale aktører.
- **Andre aktører:** Regionale Etske komiteer for medisin og helsefaglig forskningsetikk (**REK**) og Den nasjonale komité for medisin og helsefag (**NEM**).

## Datatilsynets posisjon

Følgende prinsipper legges til grunn:

- Datatilsynet ser behov for at det foretas en opprydning rundt lokale kvalitetsregistre slik at disse opprettes i samsvar regelverket. Hovedproblemet er trolig manglende bevissthet rundt kravene og manglende styring fra ledelsen. Datatilsynet oppfatter ikke at det er motvilje i organisasjonene til å etterleve regelverket.
- Det er ønskelig at det settes rammer i regelverket for behandlinger som forventes å finne sted ved helseforetakene. Derfor er det naturlig å avklare grensene for hva som er forskning, alternativt at det settes klarere rammer for kvalitetssikring utover det som tillates etter helseforskningslovens § 26. Datatilsynet startet påvirkningen i arbeidet høsten 2010 gjennom en kontroll med et større helseforetak.
- For nasjonale og regionale helseregistre legger Datatilsynet til grunn de samme prinsippene som for Sentrale helseregistre. I dag er det en rekke nasjonale kvalitetsregistre basert på samtykke, som fungerer godt. Knyttet til regelverksutvikling rundt fellesregistermodellen mener Datatilsynet at man ikke bør gå bort fra samtykke for de tilknyttede kvalitetsregistrene.

## Datatilsynets strategi

Datatilsynet skal:

- gjennomføre enkelte kontroller med helseforetak med lokale kvalitetsregistre som tema
- avklare rekkevidden for regelverket ved aktiv kontakt med Helse- og omsorgsdepartementet og Helsedirektoratet
- ha dialog med de etiske komiteene (REK og NEM) om rammene for helseforskningsloven
- bidra til at reglene rundt lokale kvalitetsregistre blir kommunisert til pliktsubjektene, blant annet gjennom samhandling med SKDE

## Helseforskning

*Helseforskningsloven trådte i kraft 1. juli 2009. Et av målene med loven var å gjøre søknadsprosessen enklere og mer effektiv ved at det ble innført et hovedprinsipp om en postkasse (REK), samtidig som hensynet til forskningsdeltakeren og personvern skulle ivaretas. REK overtok i denne forbindelse oppgaver som tidligere lå hos Datatilsynet (konsesjon for behandling av helseopplysninger) og Helsedirektoratet (dispensasjon for taushetsplikt og godkjenning for opprettelse av forskningsbiobank). Helseforskningsloven skulle være en videreføring av gjeldende rett, ikke medføre en lemping av personvern hensynet. Datatilsynet og Helsetilsynet har tilsynskompetanse etter helseforskningsloven.*

## Utfordringer

Intensjonen med helseforskningsloven var blant annet at personvernet skulle ivaretas like godt og at loven ikke skulle medføre en lemping på personvernrettighetene. Erfaringene så langt kan tyde på at en viss justering av forvaltningspraksis. Det er flere eksempler på saker der Datatilsynet og Personvernemnda har gitt avslag, men der det nå er gitt tillatelse av REK. Det er i slike sammenhenger ikke begrunnet hvorfor man har landet på en lempeligere praksis.

REKene skal etter innføringen av helseforskningsloven gjøre de vurderingene Datatilsynet og Helsedirektoratet tidligere gjorde i tillegg til de etiske. Rollen som et uavhengig forvaltningsorgan ble ny med helseforskningsloven. Det har vært begrenset kompetanseoverføring til REK fra Datatilsynet og Helsedirektoratet på personvern og informasjonssikkerhet. Følgende utfordringer er identifisert:

- Det er behov for kompetanseoverføring til REKene og NEM om personvern og informasjonssikkerhet.
- REKenes kompetanse etter helseforskningsloven må klargjøres.
- Datatilsynets tilsynskompetanse etter helseforskningsloven må klargjøres.
- Det er behov for bedre veiledninger om informasjonssikkerhet, identitetshåndtering, koblingsprosedyrer, informasjonsplikten, webbasert innhenting av sensitive opplysninger med videre.

## Aktørene:

- **Regionale Etiske komiteer for medisin og helsefaglig forskningsetikk (REK)** består av syv regionale komiteer som er satt sammen av personer med ulik fagbakgrunn, lekrepresentanter og representanter for pasientforeninger. Komiteene oppnevnes av Kunnskapsdepartementet for fire år om gangen.
- **Den nasjonale komité for medisin og helsefag (NEM)** avgjør klager på REKenes vedtak og skal sikre likebehandling.
- **Helse og omsorgsdepartementet** har fortolkningsansvaret for helseregisterloven og helseforskningsloven. Departementet har også utarbeidet en veileder for helseforskningsloven.
- **Kunnskapsdepartementet:** REKene er administrativt underlagt Kunnskapsdepartementet, men er et uavhengig forvaltningsorgan.

- **Helsetilsynet og Datatilsynet** har tilsynskompetanse etter helseforskningsloven.
- **Helsedirektoratet** koordinerer arbeidet med Norm for informasjonssikkerhet i helse-, omsorgs-, og sosialsektoren (Normen). Denne omfatter alle krav som må tilfredsstilles for å oppfylle lov og forskriftskrav. Alle aktører i sektoren som er tilknyttet Norsk Helsenett er avtalerettslig forpliktet til å følge Normen. Direktoratet har laget en egen veileder om helseforskning i regi av normarbeidet. Direktoratet vil være en viktig kanal for veiledning av forskningsmiljøene.
- **Andre aktører:** Sentrale helseregisterforvaltere og Forskningsansvarlige.

## Datatilsynets posisjon

Følgende prinsipper legges til grunn:

- Personvernet skal ivaretas like godt gjennom helseforskningsloven som tidligere, slik Stortinget forutsatte da loven ble vedtatt.
- Datatilsynet skal jobbe for at borgernes autonomi og personvern ivaretas i helseforskningsprosjekter.
- Det er sentralt at deltakere i helseforskningsprosjekter blir gitt god informasjon. Dette er en forutsetning for at deltakerne kan ivareta egen autonomi og kunne ta i bruk øvrige rettigheter i personvernregelverket.
- Det bør utredes og etableres gode reservasjonsløsninger. Disse bør være enkle, lett tilgjengelige, og godt kjent i befolkningen.
- Personvern og informasjonssikkerhet må bli vurdert og ivaretatt tidlig i prosessen hos forskningsansvarlig og REK. Det er uheldig dersom lovbrudd først blir avdekket av Datatilsynet på tilsyn fordi krenkelsen da i mange tilfeller allerede har skjedd.

## Datatilsynets strategi

Datatilsynet skal

- ta initiativ til kompetanseoverføring til REK og NEM - særlig gjelder dette grenseflaten mellom helseregisterloven og helseforskningsloven, informasjonspplikt, informasjonssikkerhet, gjennomføring av registerkoblinger / identitetshåndtering og webbasert innhenting av sensitive opplysninger med videre
- gjennomføre et gitt antall kontroller (på bakgrunn av erfaringer fra tilsyn i 2010 kan det være fornuftig å ta utgangspunkt i utleveringer til helseforskningsprosjekter fra sentrale helseregistre for eksempel fra Norsk pasientregister)
- tilbakeføre kunnskap til REK og NEM etter kontroller
- bidra til å utvile bedre veiledere overfor helseforskningsmiljøet gjennom arbeidet med Normen
- ha dialog med Helse- og omsorgsdepartementet, Kunnskapsdepartementet, Helsetilsynet og REK og NEM

## Lokale behandlingsrettede helseregistre

*Med lokale behandlingsrettede helseregistre menes her elektroniske pasientjournaler som den enkelte databehandlingsansvarlige oppretter for dokumentasjon av den helsehjelp som ytes. Med innføringen av ny kommunehelselov utvides denne til også å omfatte sosial- og omsorgstjenester. Begrepet omfatter også en rekke registre som dannes ved bruk av elektronisk utstyr som inngår i helsehjelpen.*

### Utfordringer

Datatilsynet ser konfidensialitetsvern (tilgangsstyring og logging) som en hovedutfordring. Dette er behandlet i et eget strategidokument om tilgangsstyring.

#### Generelle utfordringer

Det hevdes i mange tilfeller at personvernet prioriteres over "pasientvernet" i helsesektoren, og at Datatilsynet hindrer enkle løsninger for tilgang og samhandling. Det er en kommunikasjonsutfordring at løsningene i sektoren må være lovlige, og at det er mulig å lage løsninger som både ivaretar de helsefaglige behovene og personvernet.

Det er stor tro på endring og forbedring av arbeidsprosessene i sektoren, og ofte er IKT et virkemiddel for å oppnå dette. Det loves ofte at nye IKT-løsninger både kan løse nye oppgaver og ivareta personvernet, mens personvernet i praksis nedprioriteres i utformingen.

Samhandlingsløsninger er sentralt i sektoren for å bedre pasientbehandlingen. Dette medfører også personvernutfordringer, blant annet for pasientens kontroll med og tilgang til opplysningene, og for klarhet om virksomhetenes ansvar for opplysningene.

#### Helseforetakene med videre

De regionale helseforetakene er databehandlere for helseforetakene i sin region. Dette har medført bruk av felles journalsystemer, og at de forventede skillene mellom ulike behandlingsansvarlige utfordres.

Tilsvarende har de regionale helseforetakene, som eier av helseforetakene, tiltatt seg en vesentlig del av beslutningskompetansen som forventes å ligge hos den enkelte behandlingsansvarlige. Dette utfordrer helseforetakenes mulighet til å gjøre selvstendige valg for å etterleve regelverket.

Videre er det en utfordring at journalen hos helseforetakene består av mange systemer som i mange tilfeller ikke er godt integrert med hverandre. Utfordringer er blant annet kontroll over informasjonen, kvalitet, og mulighet for at pasienten kan få innsyn.

#### Kommunehelsetjenesten

I kommunehelsetjenesten benyttes det felles fagsystemer for administrative beslutninger om ytelser(tjenesteutmåling) og for journalføring av helsehjelpen. Tjenestene spenner over svært ulike former for helsehjelp som tjenestemottakeren vil oppleve som uavhengige tjenester, som

eldreomsorg, oppfølging av barn- og unge og oppfølging av utsatte grupper. Bruk av felles systemer innebærer fare for formålssammenblanding og bruk av overskuddsinformasjon. Det kan også gi utfordringer med å etablere en god tilgangsstyring i systemene. Det altomfattende fagsystemet på kommunalt nivå har etter Datatilsynets syn, en uoverskuelig personvernulempe.

I kommunesektoren er det en økende grad av tjenesteutsetting til andre offentlige eller private aktører. I mange tilfeller ønsker kommunene at disse bruker kommunens fagsystem. Dette er i konflikt med eksisterende regelverk, og det er behov for lovlige løsninger som både ivaretar personvernet og de praktiske behov ved tjenesteutsetting.

For legevakten som ofte er felles for flere kommuner eller er samlokalisert med sykehus, har det vært en utfordring at legevakten har tilgang til en svært begrenset mengde opplysninger. Dette problemet løses trolig i det vesentlige gjennom regelverksendringene knyttet til kjernejournal og tilgang på tvers.

### **Primærhelsetjenesten**

Primærhelsetjenesten er i det vesentlige organisert ved at flere enkeltpersonforetak eller lignende arbeider sammen i formaliserte arbeidsfellesskap. Dette gir uklare ansvarsforhold, og felles driftsløsninger samsvarer i dag ikke med regelverket. Det er adgang til å fastsette rammer for slike arbeidsfellesskap gjennom forskrift. Dette arbeidet har ikke blitt prioritert.

Det gir vesenlige utfordringer for informasjonssikkerheten, spesielt med hensyn til skadelig programvare og bruk av usikrede tjenester i samhandling med pasienten, at helsefaglige systemer knyttes nært opp mot Internett.

Virksomhetene er små og trenger god veiledning, aktive foreninger og tilpassede tjenester for å etterleve regelverket. Etter hvert som virksomhetene bringes inn i prosesser som krever samhandling over Norsk Helsenett får de tilgang til slikt veiledningsmaterieell. Grupper som psykologer, fysioterapeuter, alternative behandlere etc. er ikke inkludert per i dag, mens allmennlegene og tannlegene kan nå sies å være innenfor. Norm for informasjonssikkerhet er sentral for veiledning.

### **Aktørene:**

- **Helse- og omsorgsdepartementet** er sentral i regelverksutvikling som berører alle de tre områdene. Pågående viktig arbeid er forskrift for formaliserte arbeidsfellesskap og ny kommunehelsetjenestelov. I tillegg kommer helseinformasjonssikkerhetsforskriften som vil tre i kraft i løpet av 2012.
- **Helsedirektoratet** er sentral for alle områder, spesielt gjennom ansvaret for Norm for informasjonssikkerhet.
- **Norsk Helsenett** er i kontakt med alle virksomheter som kobles til nettet. Dette medfører at de er en sentral part for å bevisstgjøre virksomhetene, spesielt i primærhelsetjenesten.
- **Andre aktører:** Helsetilsynet, Kommunenes Sentralforbund, Profesjonsforeninger (primærhelse), Norsk Helsenett, Nasjonal IKT, Regionale sikkerhetsfora, Primærhelsetjenesten (legekontor, tannleger, psykologer med videre), Kommunale helsetjeneste (omsorg, legevakt, skolehelse med videre), IT-tjenestene (databehandlere og leverandører), Spesialisthelsetjenesten (HF, private HF, RHF og avtalespesialister).

## Datatilsynets posisjon

Følgende prinsipper legges til grunn:

- Det er grunnleggende at aktørene anskaffer løsninger som både ivaretar de helsefaglige behovene og personvernet. Dette inkluderer selve journalsystemene og løsninger for drift og kommunikasjon.
- Det er viktig at regelverket blir fulgt på en lojal måte. Det må være rom for dialog om ønsket utvikling fremfor at aktører bevisst velger å "utfordre" eksisterende regelverk.
- For virksomheter med begrenset kompetanse, spesielt i primærhelsetjenesten, må det legges til rette for etterlevelse ved at det utarbeides tilpasset veiledningsmateriell.

## Datatilsynets strategi

### Generelt skal Datatilsynet

- utvikle et tettere samarbeid med leverandører av pasientjournaler. Formålet er å bidra til at det utvikles systemer hvor personvernet kan ivaretas på en god måte. Tilsynet skal bidra til at det etableres en godkjennings- eller sertifiseringsordning for sektoren, og delta i fastsettelse av krav for slik godkjenning;
- videreføre deltakelse og arbeid knyttet til Norm for informasjonssikkerhet (Normen) på nye områder. Normen har gitt et stort løft i sektoren. Tilsynet er også opptatt av at produktene som leveres fra Norsk Helsenett underbygger etterlevelse av Normen;
- stille seg til rådighet for sektorens egne arenaer hvor personvern diskuteres. Herunder helseforetakenes regionale sikkerhetsfora, Kommunal informasjonssikkerhet (KINS) for kommunene og fagsamlinger i primærhelsetjenesten.

### For primærhelsetjenesten spesielt skal Datatilsynet:

- identifisere delsektorer som har behov for å løftes med hensyn til regelverksetterlevelse, og gjennomføre et begrenset antall tilsyn hos disse. Funn skal benyttes som grunnlag for videre oppfølging og veiledning fra egen bransjeorganisasjon. Datatilsynet skal bistå i utarbeidelse i veiledningsmateriale, og hvor det er naturlig bør veiledningsmateriale knyttes mot Norm for informasjonssikkerhet. Strategien har tidligere vært vellykket ovenfor allmennleger og tannleger;
- overfor departementet kommunisere viktigheten av at det utarbeides forskrift om formaliserte arbeidsfellesskap. Dagens praksis hvor tilsynet ikke håndhever gjeldende rett, men avventer bebudet regelverksutvikling, er ikke tilfredsstillende.

## Tilgangsstyring i journalsystem

*Det er store utfordringer med å balansere hensynet til helsepersonellens behov for nødvendig informasjon og pasientens integritetsvern, ved at det ikke gis større tilgang til journalen enn nødvendig. På den ene side skal helsepersonell ha tilgang til relevant informasjon om pasientene de behandler, på den annen side må kombinasjonen av gitt tilgang og kontrollsystemer bidra til å forhindre misbruk av systemet. Erfaringer har vist at det er store utfordringer med å balansere de ulike hensyn.*

### Utfordringer

Tilgang til relevante helseopplysninger er meget viktig for å kunne yte fullgod helsehjelp. Følgende utfordringer er identifisert:

- Det er mangelfull bruk av tilgangsstyring i journalsystem. Tilgang gis ofte for vid, over en for lang tidsperiode, en betydelig informasjonsdybde, og for en stor populasjon.
- Sektoren har kommet kort med å begrense tilgangen til den som faktisk er involvert i behandlingen av pasienten, såkalt beslutningsstyrt tilgangsstyring.
- Selv om logging er i ferd med å komme på plass mange steder, er bruk av logger i stor grad fraværende. Dette skyldes manglende funksjonalitet eller vilje.

### Aktørene:

- Helseforvaltningen, spesielt **Helse- og omsorgsdepartementet (HOS), Helsedirektoratet (HD) og Statens Helsetilsyn (SH)** er viktige parter i arbeidet med å sette klare rammer for sektoren. Uten at det settes nærmere rammer for hva som er akseptabel grad av tilgangsstyring, er det liten grunn til å tro at en vil lykkes. Bruk av standardisering og Norm for informasjonssikkerhet er viktige verktøy i denne sammenhengen.
- **Leverandører av elektroniske journalsystem** er viktige aktører. Dersom verktøyet ikke er anordnet for en god tilgangsstyring, vil det være vanskelig for de øvrige aktørene å få realisert gode løsninger.
- Innen **primærhelsetjenesten** er de små medisinske enhetene i en utfordrende situasjon. De har ofte et svakt driftsmiljø og må støtte seg på leverandørene.
- **Norsk Helsenett** er en viktig aktør. De leverer tilknytning til ytre nett, og er en viktig part for sikkerhet.
- **Brukerne av elektroniske journalsystemer** deler seg inn i tre grupper: de store foretakene, kommunene, og de mindre medisinske enhetene. De to førstnevnte har størst utfordringer med hensyn til tilgangsstyring på grunn av de mange ansatte og sammensatte arbeidsprosessene. De mindre medisinske enhetene har et begrenset brukermiljø, hvilket også begrenser tilgangsproblematikken. Likevel, mangelfulle kontrollmekanismer reduser behandlende helsepersonell sin mulighet for å avdekke "snoking" fra samarbeidende personell.
- **Bransjeorganisasjoner** som Legeforeningen og Tannlegeforeningen, er sentrale parter for å nå primærhelsetjenesten.

## Datatsynets posisjon

Følgende prinsipper legges til grunn:

- Tilgang til journalopplysninger skal begrenses til det nødvendige og være i samsvar med taushetsplikten. Datatsynet støtter seg på helseforvaltningen i vurderinger av taushetsplikten.
- Det bør etableres mekanismer for tilgangsstyring slik at den er tilpasset sektorens dynamiske hverdag (beslutningsstyrt tilgangsstyring), slik at tilgangen følger pasientforløpet.
- Det må etableres en tilfredsstillende kontroll med hvordan tilgang benyttes.
- Konfidensialiteten må ikke utelatende baseres på loggkontroll.
- Det er behov for klarere rammer for leverandører og brukere av journalsystemer om hva som er akseptabelt å gi av tilgang innefor rammene av taushetsplikten.
- Ulike tiltak kan balanseres og til sammen skape en akseptabel tilgangsstyring.
- I mindre helsevirksomheter må det etableres mekanismer som er tilpasset størrelse og organisering. Regulering av dagens praksis med tilgang mellom samarbeidende virksomheter, gjennom forskift avventes.
- Forvaltere av elektronisk pasientjournal må balansere tilgang til helseopplysninger med tilfredsstillende personvern. Dette kan gjøres ved at følgende parametre påvirkes:
  - antallet medarbeidere som har tilgang
  - tidsintervallet slik tilgang gis for
  - populasjonen det gis tilgang til
  - informasjonsdybden den enkelte får
  - de operative kontrollmekanismene

## Datatsynets strategi

Datatsynet skal

- bidra til at sektoren får klarere rammer for hva som kan gis av tilganger. Dette gjelder helseforetak og kommuner, så vel som primærhelsetjenesten. Arbeidet må føres av HOD og Helsedirektoratet, og Datatsynet vil bidra. Innsatsområder kan være standardisering, rundskriv og Norm for informasjonssikkerhet;
- følge forsøksprosjektene for logganalyse nøye, og bidra i prosjektene ved behov;
- kommunisere klart ovenfor partene viktigheten av at tilgangsstyringen knyttes nærmere til pasientforløpet ved bruk av beslutningsstyrt tilgangsstyring;
- veilede publikum om rett til innsyn i logger, samt om rett til å gjennomføre sperringer i journaler;
- jobbe aktivt overfor leverandørene av journalsystemer for å bygge opp kunnskap om disse, samt påvirke hvordan de utvikles videre;
- arbeide tett mot Helsedirektoratet for å styrke Helsenormen, både i forhold til innholdet samt utbredelse av denne;
- føre tilsyn med tilgangsstyring i journalsystemer, fortrinnsvis i samarbeid med Helsetilsynet;
- samarbeide tettere med de regionale helseforetakene for å understøtte prosessen med å få til bedre kontrollmekanismer for journalsystemene.

## Tilgang på tvers av helseforetak og kjernejournal

*Dagens pasientbehandling er preget av dynamikk og samarbeid, og gjør det nødvendig med utveksling av en betydelig mengde pasientopplysninger. Det er derfor åpnet for tilgang på tvers av helseforetak og satt i gang et prosjekt for å etablere elektronisk kjernejournal. Det er viktig at borgernes krav på konfidensialitet ivaretas og at de lovmessige skranker for samhandling som er vedtatt, faktisk blir ivaretatt. Dessuten må elektronisk kjernejournal i størst mulig grad ivareta borgernes krav på autonomi og selvbestemmelse.*

### Utfordringer

Stortinget åpnet i Ot.prp. nr. 51 (2008-2009) for å gi tilgang på tvers av helseforetak. Høsten 2010 sendte Helse- og omsorgsdepartementet på høringen et forskriftsforslag om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre. Forskriften ble fastsatt i statsråd 24. juni 2011 og trer i kraft i 2012. Helsedirektoratet la i januar 2011 fram en rapport om nasjonal kjernejournal. Det ble også fattet en politisk beslutning om at det skal etableres en slik journal. I forslaget legges det opp til at pasienten kan reservere seg mot å la sine opplysninger registrere i kjernejournalen, men det forslås samtykke for bruk av journalen.

I en del tilfeller er det behov for tilgang på tvers av helseforetak. Det er stor mobilitet i moderne medisinsk behandling og det er ikke uvanlig at for eksempel en hjertepasient er til behandling ved tre til fire forskjellige helseforetak.

Dagens pasientjournaler er ikke strukturert slik at en lege på et sykehus kan få tilgang på kun relevant og nødvendig informasjon for å yte helsehjelp til den enkelte pasient fra et annet helseforetak. Dagens statiske journalstruktur er med andre ord ikke tilpasset et dynamisk behandlingsforløp. Dette innebærer en klar fare for personvernet ettersom det i mange tilfeller vil bli gitt tilgang til mer informasjon om pasienten enn det tjenestelige behov tilsier. Men det er også et problem sett med pasientøyne fordi dette innebærer en mulighet for at helsepersonell ikke får tilgang til relevant informasjon i tide.

Privatisering av helse og omsorgstjenester har ført til at institusjoner deler journalsystem av praktiske og kanskje særlig økonomiske årsaker. Dette øker risikoen for at et ubestemt antall personer har tilgang til opplysninger om den enkelte pasient uten at noen har reell kontroll over hvem som har tilgang til hva.

Elektronisk kjernejournal kan til en viss grad avhjelpe behovet for tilgang på tvers. Samtidig skaper elektronisk kjernejournal utfordringer for personvernet. I den foreslåtte løsningen legges det blant annet opp til en kombinasjon av reservasjon og samtykke. Særlig i de situasjoner der det foreligger en dialog mellom pasient og helsepersonell, ser Datatilsynet det som naturlig at det også legges opp til at kjernejournalen etableres på et samtykke.

Dagens lov og forskrift er slik Datatilsynet ser det, ikke i tilstrekkelig grad veiledende for helseforetak når de skal åpne for tilgang på tvers. Tilsynet har derfor etterlyst en nærmere konkretisering av *hvordan* det skal åpnes for tilgang, for eksempel i rundskrivs form.

## Aktørene:

- **Helse – og omsorgsdepartementet (HOD)** er en sentral aktør fordi de sitter med det overordnede ansvar for lov- og regelverksutviklingen på området og dessuten i stor grad styrer pengene. I tillegg er alle viktige politiske prosesser forankret i HOD.
- **Helsedirektoratet** iverksetter helsepolitikken og er en sentral premissleverandør til HOD og øvrige aktører i helseforvaltningen. I tillegg har Helsedirektoratet operativt ansvar for kjernejournal-prosjektet.
- **Helsetilsynet** er en viktig aktør når det gjelder oppfølging av om reglene etterleves, typisk i forbindelse med tilsyn.
- **Legeforeningen** og andre **profesjonsorganisasjoner og pasientforeninger** er viktige aktører og jobber aktivt for å fremme sine respektive interesser overfor sentrale aktører i helseforvaltningen.
- **Utviklere av journalsystemer** sitter i en viktig posisjon og kan bidra til å gi aktørene i helsesektoren de rette verktøyene som sikrer tilstrekkelige kontrollmekanismer.

## Datatilsynets posisjon

Følgende prinsipper legges til grunn:

- Stortingets forutsetninger for å åpne på tvers må ivaretas, blant annet gjennom at det kun åpnes for tjenestelig adgang til relevante opplysninger.
- Det skal jobbes for at det vedtas retningslinjer på nivå under forskrift, og for at forskriften ikke trer i kraft før systemene er på plass og journalene strukturert.
- Det skal jobbes for at borgerens autonomi og selvbestemmelse ivaretas i en kjernejournal-løsning, og at det gis regler om logging og innsyn.
- Det er viktig at Nasjonal kjernejournal etableres som et eget nasjonalt behandlingsrettet helseregister, og ikke bygges opp som en distribuert løsning som kun gjør oppslag i andre sentrale helseregistre som for eksempel Reseptformidleren, Norsk pasientregister med videre.
- Det skal jobbes for at det er teknisk mulig for helseforetakene å oppfylle regelverkets krav.
- Det skal jobbes for at pasientene blir gjort kjent med oppslag som er gjort i hans eller hennes kjernejournal.

## Datatilsynets strategi

Datatilsynet skal

- ha tett dialog med sentrale aktører i helseforvaltningen, som Helse- og omsorgsdepartementet, Helsedirektoratet og Helsetilsynet
- ha tett dialog og samarbeid med profesjonsforeninger og pasientforeninger for i fellesskap å påvirke sentrale aktører slik at regelverket om å få tilgang på tvers og kjernejournal blir best mulig

For tilgang på tvers av helseforetak skal Datatilsynet

- ha dialog med HOD for å påvirke departementet til å lage rundskriv eller lignende på nivå under forskrift, og jobbe for at regelverket blir best mulig

- ha god dialog med leverandører av journalsystemer ut fra en målsetning om å bygge godt personvern inn i framtidige tekniske løsninger
- gjennomføre aktivt tilsynsarbeid for eksempel tre måneder etter at forskriften har trådt i kraft, gjerne i samarbeid med Helsetilsynet

For arbeidet med elektronisk kjernejournal skal Datatilsynet

- delta aktivt i Helsedirektoratets arbeid med elektronisk kjernejournal ved jevnlige møter og innspill
- jobbe for løsninger som i best mulig grad ivaretar pasientens autonomi og selvbestemmelse, både i bruks- og innhentingsfasen av kjernejournal - dette innbefatter også innsynsrett og mulighet for å korrigere feil
- jobbe for at datakilder og datainnsamling skjer på en god måte personvernmessig
- jobbe for god informasjonssikkerhet i løsningen og for et godt system for logging av oppslag
- jobbe for samtykkeløsning der det er dialog mellom pasient og helsepersonell, at en eventuell reservasjonsløsning blir godt kjent blant borgerne og for at den skal bli enkel å administrere

## Ny teknologi i helsevesen og omsorgssektoren

*Bruk av IKT i helsevesenet står høyt på den politiske dagsorden. Helseportalen helsenorge.no er lansert og bruk av velferdsteknologi vil i stadig større grad supplere personlig kontakt mellom behandler og pasient. Brukt riktig kan dette føre til styrket personvern for borgerne, men det reiser samtidig utfordringer for pasientenes integritet og selvbestemmelse. Det er særlig viktig at godt personvern integreres i teknologien tidlig i utviklingsfasen.*

### Utfordring

Økt forventning til helsehjelp, begrenset tilgang på arbeidskraft og en stadig eldre befolkning, tvinger frem løsninger som kan bidra til et mer effektivt helsevesen. Bruk av teknologi i helsevesenet vil øke kraftig. Dette kan skape utfordringer i et personvernperspektiv, men kan i tillegg bidra til økt trygghet for pasienten og at større deler av helsehjelpen flyttes til pasientens hjem.

### Pasienten på nett

Det er et politisk ønske at kommunikasjonen mellom borger og stat skal skje elektronisk. Innen helsevesenet ser man dette blant annet ved etableringen av portalen helsenorge.no. Helseopplysninger oppleves av de aller fleste som mer beskyttelsesverdige enn andre opplysninger om en selv. Dette stiller store krav til sikkerhet i kommunikasjonsløsningene.

I den alminnelige dialogen med helsepersonell ser pasienten hvem som er ”i andre enden”. Dette er ikke alltid like klart ved elektronisk kommunikasjon.

Det er et sentralt spørsmål om hvilke typer opplysninger som skal kunne utveksles og hvilke kommunikasjonskanaler som skal kunne benyttes. For portaler er det et spørsmål om hvem som skal beslutte at opplysningene gjøres tilgjengelige. Det synes naturlig at dette bør baseres på samtykke fra pasienten.

Mobile løsninger, som diabetesmåling via mobiltelefon og håndholdte enheter for helsepersonell, innebærer også sikkerhetsutfordringer.

### Omsorgsteknologi

Velferdsteknologien er mangeartet, og noen eksempler er sporingsteknologi, fallalarmer og bruk av mobilteknologi i oppfølging av pasienter. Slike løsninger kan ivareta pasientenes helsemessige behov på en god måte, samtidig som personvernet ivaretas. Mange vil for eksempel oppleve det som mindre integritetskrenkende å avlegge en urinprøve hjemme og sende svaret elektronisk enn å gjøre det på et legekantor.

Samtidig utfordrer slik teknologi personvernet. Omsorgsteknologi kan føre til overvåking og kontroll som krenker den enkeltes personlige integritet. En del av de potensielle brukerne av omsorgsteknologi vil dessuten ha større eller mindre grad av kognitiv svikt. Det er viktig å huske at også disse personene har et krav på personvern og at deres personlige integritet respekteres.

I dag mangler det et rettslig grunnlag for å ta i bruk slike tiltak i den offentlige helse- og omsorgstjenesten uten at det foreligger samtykke fra pasientene. Gyldigheten av samtykke fra demente og andre med kognitiv svikt krever også en rettslig avklaring.

For at omsorgsteknologien skal utvikle seg på en god måte er det avgjørende at viktige personvernforutsetning er oppfylt. Valg av tiltak er sentralt. Hjelpemiddelet som tas i bruk må være minst mulig integritetskrenkende, for eksempel sporingsteknologi i sanntid framfor en fullstendig oversikt over bevegelsesmønster, alarm som utløses av pasienten selv i de tilfellene det er tilstrekkelig, og såkalte "geofences" fremfor kontinuerlig overvåking.

Det er viktig at informasjonssikkerheten er godt ivaretatt og at tilgangsstyringen er god. Det må også innføres sletterrutiner for å sikre at det ikke samles og oppbevares unødvendig informasjon om den enkelte.

Det er svært viktig at personvernvennlige løsninger bygges inn i de omsorgsteknologiske løsningene allerede fra starten.

### Aktørene:

- **Helse og omsorgsdepartementet** forvalter det sentrale lovverket på området.
- **Helsetjenesten**, særlig i kommunal sektor (for eksempel Kommunenes Sentralforbund) vil være kjøper og bruker av omsorgsteknologi.
- **Direktorat for forvaltning og IKT** er viktig i utviklingen av publikumsløsninger og som forvalter av ID-porten.
- **Leverandører av tekniske løsninger, hjelpemidler og programvare** kan blant annet bidra til utvikling av personvernvennlig teknologi.
- **Teknologirådet** besitter stor kompetanse på området og har blant annet utredet brukspotensialet for slik teknologi.
- **Helsedirektoratet** er fagansvarlig direktorat og samtalepart når det er behov for ytterligere regulering for å ivareta personvern, eller klargjøring av eksisterende regelverk.
- **Profesjonsforeninger og pasientforeninger** er en faglig ressurs i spørsmål om nytteverdi og betydning for behandlere.
- **SINTEF** driver utstrakt forskning på omsorgsteknologiområdet.

### Datatilsynets posisjon

Følgende prinsipper legges til grunn:

#### Pasient på nett:

- Pasienten må gis god informasjon om hvordan ny teknologi innen helse og omsorg påvirker den enkeltes personvern.
- Tilgjengeligheten av pasientopplysninger må i størst mulig grad baseres på samtykke.
- Det må ikke registreres mer personopplysninger enn det som er nødvendig. Hva som er nødvendig må avstemmes mot pasientens samtykke. Likevel bør det være et reelt valg med et snevrere utvalg bør være en opsjon. Eksempelvis bare det nyeste og det viktigste.
- Datatilsynet ønsker en portalløsning i motsetning til en sentral løsning hvor alt ligger samme sted. Det bør lagres minst mulig i en slik portal.

**Omsorgsteknologi:**

- Bruk av denne typen teknologi må i største mulig grad baseres på samtykke.
- Det må på plass en lovregulering for de tilfelle der bruk av omsorgsteknologi ikke kan baseres på samtykke.
- Det må på plass en lovregulering av den faktiske bruken av omsorgsteknologi, også for demente og andre som lider av kognitiv svikt.
- Det må velges en minst mulig personverninnvirkende teknologi.
- Bruken må være styrt av et definert formål og konkrete krav.
- Utviklingen av omsorgsteknologien bør bygges på prinsippet om personvernvennlig teknologi, se vedlegg III.
- Helsevesenet som bestiller må etterspørre personvernvennlige løsninger.

**Datatilsynets strategi**

## Pasient på nett - Datatilsynet skal:

- tydeliggjøre vår posisjon og våre prioriteringer overfor Helsedirektoratet vedrørende hva som bør være tilgjengelig over Internett
- tydeliggjøre våre posisjoner overfor Helse og omsorgsdepartementet og sikre at det ikke lages nye regler for hva som kan tilgjengeliggjøres over Internett, uten at det er innhentet samtykke i forkant
- sikre at det ikke legges opp til systemer som baserer seg på tvungen ordning med at alt tilgjengeliggjøres over Internett
- ta initiativ til dialog med interesse- og bransjeorganisasjoner med sammenfallende interesser som Datatilsynet

## Omsorgsteknologi - Datatilsynet skal:

- jobbe aktivt for at det kommer på plass et rettslig grunnlag for bruk av omsorgsteknologi
- samarbeide med myndigheter og interesseorganisasjoner
- ha tett dialog med leverandører av omsorgsteknologi og med ulike miljøer som driver forskning og utredning på området, som for eksempel SINTEF og Teknologirådet
- jobbe for å fremme bruken av personvernvennlig teknologi overfor utviklere av teknologiske løsninger
- jobbe for at det offentlige helsevesen stiller krav om at det skal velges mest mulig personvernvennlige teknologiske løsninger, bygd på prinsippene for innebygd personvern

## Vedlegg I: Begrepsavklaringer

**Normen:** Norm for informasjonssikkerhet i helse-, omsorgs-, og sosialsektoren. Normen omfatter alle krav som må tilfredsstilles for å oppfylle lov og forskriftskrav. Alle aktører i sektoren som er tilknyttet Norsk Helsenett er avtalerettslig forpliktet til å følge Normen.

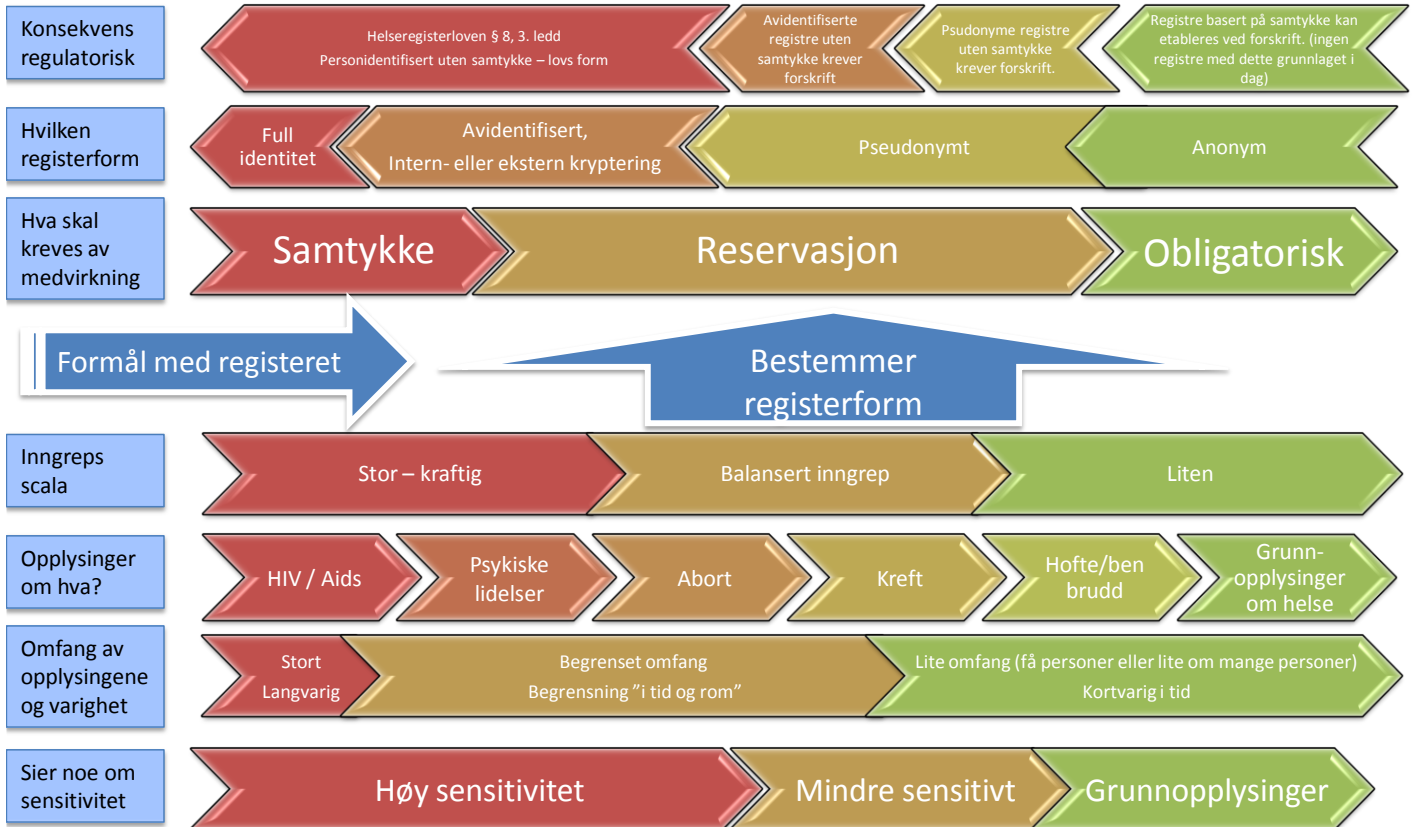
**Fellesregistermodellen:** Betegnelsen på en ny måte å organisere et sentralt helseregister på. Nasjonalt register over hjerte- og karlidelser er første helseregister av denne typen. For dette registeret innebærer modellen innebærer etablering av et sett av basisregistre med personidentifiserbare opplysninger som skal samles inn uten samtykke fra den enkelte. Basisregisteret skal bestå av utvalgte parametre fra andre sentrale helseregistre som Norsk pasientregister, Dødsårsaksregisteret og folkeregisteret på personer som har eller har hatt den sykdommen eller lidelsen registeret omhandler f eks en hjerte- eller karlidelse. I tillegg skal det i tilknytning til hvert basisregister etableres et sett av medisinske kvalitetsregistre, hvor det skal vurderes om pasienter skal kunne reservere seg mot registrering.

**Beslutningsstyrt tilgang:** Innebærer at tilgangen skal følge av en konkret beslutning om å yte helsehjelp til pasienten og være tilpasset behandlingsforløpet slik at tilgangen i størst mulig grad begrenses til helsepersonell som yter helsehjelp til pasienten. At helsepersonell selv beslutter at de skal ha tilgang er ikke beslutningsstyrt tilgangsstyring i denne sammenheng.

**Strukturerte helseopplysninger:** helseopplysninger som er organisert på en slik måte at er mulig å kun gi tilgang til et avgrenset sett av klinisk informasjon (det som er relevant og nødvendig).

## Vedlegg II: Tankemodell - registerform

### Tankemodell - registerform



## Vedlegg III – Prinsipper for innebygd personvern (privacy by design)

### **1. Proactive not Reactive; Preventative not Remedial**

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

### **2. Privacy as the Default Setting**

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, *by default*.

### **3. Privacy Embedded into Design**

*Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

### **4. Full Functionality — Positive-Sum, not Zero-Sum**

*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy *vs.* security, demonstrating that it *is* possible to have both.

### **5. End-to-End Security — Full Lifecycle Protection**

*Privacy by Design*, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

### **6. Visibility and Transparency — Keep it Open**

*Privacy by Design* seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

### **7. Respect for User Privacy — Keep it User-Centric**

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

**Datatilsynet**

*Gateadresse: Tollbugata 3, Oslo*

*Postadresse: postboks 8177 Dep*

*0034 Oslo*

*E-post: [postkasse@datatilsynet.no](mailto:postkasse@datatilsynet.no)*

*Telefon: 22 39 69 00*

*Faks: 22 42 23 50*