Personvernkonsekvensvurdering (DPIA) for administrative behandlinger ved UiO

Denne malen er utviklet på bakgrunn av kravet i personvernforordningen (GDPR) artikkel 35. Malen er i stor grad basert på Datatilsynets veiledning om personvernkonsekvensvurderinger (DPIA-er). Malen gir et bilde av momentene som bør vurderes i en DPIA. Det enkelte system eller tjeneste som benytter malen må selv konkret vurdere innhold og omfang av egen DPIA. Tabellene i malen er ikke uttømmende og må tilpasses behandlingene som omfattes av DPIA-en.

**DEL I. Vurdering av behov for DPIA**

Når må en DPIA gjennomføres?

«Dersom det er **sannsynlig** at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens **art, omfang, formål og sammenhengen den utføres i**, vil medføre en **høy risiko** for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige **før behandlingen** foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet», jf. personvernforordningen artikkel 35 nr. 1.

Kriterier som kan utløse et behov for DPIA:

1. **Evaluering eller scoring/poengvurdering**, spesielt knyttet til arbeidsresultater, økonomisk situasjon, helse, personlige preferanser eller interesser, oppførsel og atferd, lokasjon og bevegelser osv.
2. **Automatiserte beslutninger** med rettslige eller lignende følger.
3. **Systematisk overvåking** av registrerte.
4. **Særlige kategorier av personopplysninger** eller **andre sensitive personopplysninger av høy personlig karakter** (sistnevnte er spesielt knyttet til de enkeltes «friheter», men også omfatte f.eks. økonomiske opplysninger).
5. **Behandling av personopplysninger i stor skala**, som at det er et stort antall registrerte involvert, store mengder data, mange ulike tuper data, lang varighet av behandlingen, stor geografisk utbredelse av behandlingen osv.
6. **Kombinering eller sammenstilling av datasett.**
7. Personopplysninger vedrørende **spesielt sårbare registrerte** (som barn, ansatte, psykisk syke, asylsøkere, eldre, pasienter, mv.).
8. **Ny teknologi tas i bruk eller behandlingen innebærer bruk av eksisterende teknologi til nye formål**, som f.eks. bruk av biometriske data for tilgangskontroll, Internet of Things-løsninger, osv.
9. Når behandlingen i seg selv **forhindrer eller begrenser de registrertes mulighet til å utøve sine rettigheter** etter lov eller avtale, eller å bruke tjenester.

Hvis systemet eller tjenesten oppfyller to eller flere av kriteriene, kan det bety at det er nødvendig å gjennomføre en DPIA. Det må alltid gjøres en god vurdering av hvorvidt det er sannsynlig at den aktuelle behandlingen samlet sett vil medføre høy risiko for fysiske personers rettigheter og friheter etter personvernforordningen. Hvis enheten/virksomheten har gjort et godt forarbeide, har full kontroll og gjort gode vurderinger allerede, burde ikke behandlingen medføre noen risikoer, og en DPIA blir ikke nødvendig.

Leder (navn på systemeier/avdelingsleder/relevant person) har besluttet at det skal gjøres en personvernkonsekvensvurdering: Instituttleder ved Institutt for Spesialpedagogikk, Det utdanningsvitenskapelige -fakultetet, professor Ona Bø Wie

**Organisering av personvernkonsekvensvurderingen og ansvarsforhold**

Følgende personer har deltatt i gjennomføringen av personvernkonsekvensvurderingen:

|  |  |
| --- | --- |
| Navn | Stilling |
| Vasiliki Diamanti | Førsteamanuensis/Leder ved Oslo SpesialPedagogikk- og LæringsLab (Oslo SPeLL) |
| Anders Lunde | Overingeniør ved Oslo SpesialPedagogikk- og LæringsLab (Oslo SPeLL) |
|  | Utøver av behandleransvaret, UiO |
|  | Personvernombud, UiO |

**DEL II. Behandling av personopplysninger i systemet/tjenesten**

2.1 Formålet med behandlingen av personopplysninger  
Beskriv formålet med behandlingen av personopplysningene i systemet eller tjenesten. Formålene skal være spesifikke, uttrykkelig angitte og berettigede. I tråd med personvernprinsippet formålsbegrensning skal ikke personopplysninger viderebehandles på en måte som er uforenlig med formålene du angir her.

Formålet med behandlingen av personopplysninger er å kunne drifte et journal- og datalagringssystem ved Oslo SPeLL studentklinikk. Klinikkens hovedformål er å gi klinikkens praksisstudenter god opplæring i klientbehandling, samt å kunne gjennomføre best mulig vurdering og utbedring av klinikkens klienter. Klinikken klienter vil bestå av både barn og voksne.

Praksisen og behandlingen av personopplysninger ved klinikken skal være relevant for utdanningsprogrammet som tilbys ved Institutt for Spesialpedagogikk, utdanningsvitenskapelig fakultet, Universitetet i Oslo. Dette dreier seg i hovedsak om spesielle pedagogiske behov innen følgende områder:

* Språkvansker
* Kommunikasjonsvansker (hørselsrelaterte, ervervede, utviklingsmessige)
* Stemmevansker
* Talevansker: stamming og løpsk tale
* Lese- og/eller skrivevansker
* Matematikkvansker
* Adferds-, emosjonelle og sosiale vansker
* Utviklingsmessige vansker

Videre er formålet at klinikken behandler persondata i overenstemmelse med gjeldende lover, og at data kan innhentes, lagres, behandles, og slettes på en hensiktsmessig måte. Særlig gjeldende er pasientjournalloven for journalføring (Lov om behandling av helseopplysninger ved ytelse av helsehjelp). Etter Helse- og omsorgsdepartementet «Rundskriv I-6/2017 om helse- og omsorgstjenestelovgivningens anvendelse for studenter og ansatte ved utdanningsinstitusjoner» vil de viktigste momentene for klinikken være:

* Pasientjournalen er et arbeidsverktøy for helsepersonell i tilknytning til at helsehjelp gis. Journalen skal blant annet gi oversikt over hvilke tiltak som er satt i verk, herunder hvilke observasjoner og vurderinger som er gjort, samt bidra til kommunikasjon mellom helsepersonell. Journalen skal gjøre det mulig for annet helsepersonell å sette seg inn i pasientens sykehistorie dersom han/hun skal overta eller samarbeide om videre undersøkelse eller behandling av en pasient. Journalen skal også tjene som bevis og tidsnært kildemateriale i pasientskadesaker eller tilsynssaker.
* Journalen skal føres i samsvar med god yrkesskikk og skal inneholde relevante og nødvendige opplysninger om pasienten og helsehjelpen, samt de opplysninger som er nødvendige for å oppfylle meldeplikt eller opplysningsplikt fastsatt i lov eller i medhold av lov. Journalen skal være lett å forstå for annet kvalifisert helsepersonell.
* Krav til journalens innhold følger av forskriften § 8, jf. særlig bestemmelsens første og tredje ledd hvor det listes opp ulike typer opplysninger som journalen skal inneholde, forutsatt at de er "relevante og nødvendige" og at andre opplysninger "skal tas inn i journalen i den utstrekning de er relevante og nødvendige."
* I helseinstitusjoner skal det utpekes en person som skal ha det overordnede ansvaret for den enkelte journal, og herunder ta stilling til hvilke opplysninger som skal stå i pasientjournalen.
* Det skal fremgå hvem som har ført opplysningene i journalen.

2.2 Datakilder  
Kryss av for om det skal innhentes nye personopplysninger (egen datainnsamling) og/eller allerede registrerte personopplysninger.

Egen datainnsamling (systemet/tjenesten vil innhente direkte fra den opplysningen(e) gjelder).

Studentinformasjonssystem (eks FS)

FEIDE

Andre systemer  
  
Spesifiser hvilke «andre systemer» data hentes fra dersom relevant:

Klinikken vil kunne motta oversendte personopplysninger som er relevante for praksisen. Klinikken har eget nettskjema der slike dokumenter eller meldinger kan lastes opp og bli levert direkte inn til klinikkens Tjenester for sensitive data (TSD) konto.

2.3 Registrerte

Registrerte er den/de personopplysningene gjelder.  
Kryss av for hvilke kategorier av registrerte det skal behandles opplysninger om.

Studenter/elever

Ansatte

Annet (spesifiser under)

Klienter med spesialpedagogiske utfordringer som er relevante for klinikkens formål (se punkt 2.1). Personer som har en behandlingsmessig relevant tilknytning til klienten (for eksempel omsorgspersoner) kan også registreres, hvis det er i overenstemmelse med pasientjournalloven. Antall registrerte: Dette er vanskelig å forutse. Dette er avhengig av hvor mange som ønsker å benytte seg av tilbudet ved klinikken, og tilgjengelige ressurser ved klinikken.

2.4 Kategorier av personopplysninger

Kryss av for hvilke kategorier av personopplysninger som vil behandles i systemet/tjenesten.

Kategorier av personopplysninger:

Navn

Adresse

Fødselsdato

Fødselsnummer (elleve siffer)

Personfotografier

Andre opplysninger, f.eks. telefonnummer, e-postadresse, IP-adresse, demografiske variabler,   
 familieforhold.

MERKNAD: Fødselsnummer er nødvendig for å behandle digitalt samtykke. Personfotografier kan forekomme for eksempel i forbindelse med videoopptak.

Spesifiser eventuelle andre kategorier: telefonnummer, e-postadresse, kjønn.

Særlige kategorier av personopplysninger (tidligere kalt sensitive personopplysninger):

Behandler ingen særlige kategorier av personopplysninger

Evt:

Rasemessig eller etnisk opprinnelse

Politisk oppfatning

Religion

Filosofisk overbevisning

Fagforeningsmedlemskap

Genetiske opplysninger

Biometriske opplysninger med det formål å entydig identifisere en fysisk person

Helseopplysninger

Opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering

At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling

Hvis relevant, spesifiser hvilke opplysninger:

Merknad: For å drifte journalsystemet i henhold til pasientjournalloven journalen inneholde relevante og nødvendige opplysninger om pasienten. I forbindelse med språkvansker kan opplysninger om etnisk opprinnelse være relevant og nødvendig. Genetiske opplysninger kan også være relevant og nødvendig for behandling, for eksempel Downs syndrom. I forbindelse med behandling av emosjonelle og sosiale vansker kan opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, og en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling være relevant og nødvendig. I tillegg behandles opplysninger som er relevante for klinikkens formål (se punkt 2.1).

2.5 Behandling av personopplysninger

Med «behandling» menes enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger. Kryss av for hva som skal gjøres med personopplysningene, og eventuelt spesifiser. Behandlingene må være i samsvar med de oppgitte formål i 2.1.

Innsamling

Lagring

Sammenstilling, kobling

Analysering

Utlevering ved overføring

Tilgjengeliggjøring

Sletting, anonymisering

Skjerming/avidentifisering

Annet (spesifiser under)

MERKNAD 1 - Innsamling:

Personopplysninger blir innsamlet i forbindelse med rekrutering av klienter ved at interesserte sender elektronisk søknad i form at et TSD nettskjema via klinikkens hjemmeside.

Personopplysninger blir også innsamlet ved klientmøter på klikkens lokaler der samtaler og undersøkelser gjennomføres. Videoopptak og lydopptak av møter kan gjennomføres. Relevante opplysninger noteres på papir og/eller direkte på datamaskin på klinikkens TSD konto (se om lagring under).

MERKNAD 2 – Lagring:

Studentklinikken har en egen TSD konto som brukes til lagring og føring av journal, lagring av video-opptak, test-resultater, info fra TSD-nettskjema, og annen lagring. Det er kun klinikkenes leder, faste ansatte, og TSD-administratorer fra Universitetets senter for informasjonsteknologi (USIT) som har ubegrenset tilgang til klinikkens data. Veiledere og studenter har kun mulighet til å få tilgang til data for sine spesifikke klinikk-klienter, i egne mappe-områder. Veileder eller studenten må de søke om dette, ved å sende inn nettskjema. Søknader blir godkjent av klinikkenes ansatte. Data som omhandler klinikk-klienter skal aldri oppbevares eller behandles noe annet sted enn i TSD mappe-området til den enkelte klient.

Arbeidsnotater fra forsamtaler og notater fra terapitimer skal oppbevares i låsbart arkivskap på klinikkens lokaler til de skannes, eller skrives inn til TSD systemet. Dette må skje ikke senere enn 1 dag etter samtale. Aribeidsnotater skal være avidentifisert, dvs. at det ikke skal inneholde direkte personidentifiserbare opplysninger.

Endelige journaloppføringer gjøres i Microsoft Word, og dokumentet/journalen for hver bruker skal føres inn i et Word-dokument med navn «JournalXXX.docx», der xxx er det samme tre-siffrede tallet som i navnet på mappa. Hvis fila ikke eksisterer fra før, må det opprettes den i riktig mappe. Journalen føres fra topp til bunn. Det vil si at etter det første notatet, skrives alle påfølgende notat inn i det samme dokument under forrige notat.

MERKNAD 3 - Sammenstilling, kobling:

Overførsels av personopplysninger fra andre parter kan gjøres ved å bruke et TSD nettskjema som sender opplysninger direkte inn til klinikkens TSD konto. Dette kan for eksempel være opplysninger som er relevante for studentens arbeid ved klinikken. Klinikkens ansatte overfører dette til spesifikt TSD mappe-område for klienten.

MERKNAD 4 – Analysering:

Tjenestene klinikken tilbyr inkluderer vurdering/testing av klienter for å identifisere vanskelighetsområder og korte programmer for utbedring/terapi hvor studentene jobber under nøye tilsyn av en kliniker. Det primære formålet med studentklinikken er opplæring av studenter. Derfor blir data analysert.

MERKNAD 5 - Utlevering ved overføring:

Som hovedregel skal ikke personopplysninger utleveres til ekstern virksomhet/institusjon. Personopplysninger kan utleveres til ekstern institusjon hvis personen henvises videre for behandling. Etter Helsepersonelloven § 25 kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp og om pasienten ikke motsetter seg det

MERKNAD 6 - Tilgjengeliggjøring:

Tilgjengeliggjøring av journaldata gjøres i henhold til pasientjournalloven, og/eller etter avtalen fra klientens samtykkeskjema. Se merknad 5.

MERKNAD 7 – Avidentifisering og sletting:

På klinikkens TSD område er det opprettet én mappe for hver enkelt klient. Mappe-navnene er anonymisert på formen «xxx», der xxx består av et tre-sifret tall fra 001-999. Hver enkelt mappe representerer én klient, og inneholder klientens data. Alle arbeidsnotater skal være avidentifiserte.

Sletting og endring av data gjøres i henhold til pasientjournalloven og andre gjeldende lover. Tidligere innskrevne notater skal IKKE slettes, mee unntak av at a) opplysningene er feilaktige eller misvisende og føles belastende for den de gjelder; b) opplysningene er åpenbart ikke er nødvendige for å gi pasienten helsehjelp. § 43 av Helsepersonelloven tilsier at opplysningene kan slettes fra journalen dersom dette er ubetenkelig ut fra allmenne hensyn, ikke strider mot bestemmelser i arkivloven § 9 og §18. Dersom krav om sletting avslås, skal kravet om sletting og begrunnelse for avslaget nedtegnes i journalen.

2.6 Lagringssted og lagringsmedier

Angi hvor og hvordan personopplysningene skal lagres og håndteres.

Fellesområde

UiO Nettskjema

UiO ePhorte

UiO HR-portalen

Annet (spesifiser under)

Lagres på TSD – Tjenester for sensitive data

2.7 Dataansvarlig, datatilgang og databehandlere

2.7.1 Dataansvarlig og personer med datatilgang

Systemeier/dataansvarlig: Instituttleder ved Institutt for Spesialpedagogikk, Det utdanningsvitenskapelige -fakultetet, professor Ona Bø Wie

Følgende personer/persongrupper vil ha tilgang til data i systemet eller tjenesten:

|  |  |  |
| --- | --- | --- |
| Navn på person/persongruppe | Rolle/funksjon | Tilhørighet |
| Førsteamanuensis Vasiliki Diamanti | Leder ved Oslo SpesialPedagogikk- og LæringsLab (Oslo SPeLL) | Institutt for spesialpedagogikk, utdanningsvitenskapelig fakultet |
| Anders Lunde | Overingeniør ved Oslo SpesialPedagogikk- og LæringsLab (Oslo SPeLL) | Institutt for spesialpedagogikk, utdanningsvitenskapelig fakultet |
| Ansettelse pågår | Vitenskapelig assistent ved Oslo SpesialPedagogikk- og LæringsLab (Oslo SPeLL) | Institutt for spesialpedagogikk, utdanningsvitenskapelig fakultet |
| TSD-administratorer fra Universitetets senter for informasjonsteknologi (USIT) | TSD-administrator | Universitetets senter for informasjonsteknologi (USIT) |
| Klinikkens studenter | Student ved klinikken | Institutt for spesialpedagogikk, utdanningsvitenskapelig fakultet |
| Veiledere ved klinikken | Veileder for klinikkens studenter | Institutt for spesialpedagogikk, utdanningsvitenskapelig fakultet, eller andre relevante institusjoner. |

Dersom personopplysninger skal overføres eller på annen måte deles med ekstern virksomhet/institusjon, må punkt 2.7.2 om databehandler fylles ut.

2.7.2 Databehandler

Følgende virksomheter vil fungere som databehandlere for systemet eller tjenesten.

Dersom det benyttes databehandler(e), fyll inn informasjon:

|  |  |  |
| --- | --- | --- |
| Virksomhet | Rolle/funksjon | Land |
|  |  |  |
|  |  |  |

Hvordan skal personopplysninger utleveres til ekstern virksomhet/institusjon?

Som hovedregel skal ikke personopplysninger utleveres til ekstern virksomhet/institusjon. Personopplysninger kan utleveres til ekstern institusjon hvis personen henvises videre for behandling. Etter Helsepersonelloven § 25 kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp og om pasienten ikke motsetter seg det.

For hver databehandler skal det godtgjøres at de gir tilstrekkelige garantier for at behandlingen oppfyller kravene i personvernforordningen og vern av den registrertes rettigheter.

For databehandler(e) er følgende oppfylt:

Databehandleravtale som oppfyller personvernforordningens krav

Mottatt beskrivelse av tekniske og organisatoriske tiltak

Mottatt oversikt over underleverandører hvis relevant

2.7.3 Overføring av personopplysninger til andre land

Det overføres ikke opplysninger ut av Norge, eller til databehandlere med utenlandsk lagring.

Hvis relevant, kryss av hvis personopplysninger skal utleveres/overføres til:

Personer/institusjoner utenfor Norge

Tredjestater (utenfor EU/EØS)

Internasjonale organisasjoner

Dersom personopplysninger skal overføres til tredjestater og/eller internasjonale organisasjoner, må det beskrives hvordan pliktene etter kapittel V i personvernforordningen skal oppfylles.

Overføringene vil skje på følgende grunnlag:

Beslutning om at det aktuelle land har tilstrekkelig beskyttelsesnivå

Overføringen er omfattet av nødvendige garantier, slik som EUs standardavtaler, beskriv under:  
 [Hvis relevant, fyll inn hvilke(n) nødvendige garantier som benyttes.]

Unntak for særlige situasjoner, beskriv under:  
 [Hvis relevant, fyll inn hvordan personvernforordningen artikkel 49 er oppfylt.]

Overføringen er underlagt bindende virksomhetsregler, slik som registrering under Privacy Shield  
 [Hvis relevant, fyll inn hvilke bindende virksomhetsregler som benyttes.]

Hva er det rettslige grunnlaget for overføring utenfor EU/EØS? [Fyll inn hvis relevant.]

Redegjør for hvordan personopplysningene overføres og lagres utenfor EU/EØS: [Fyll inn hvis relevant.]

**Del III. Rettslig grunnlag for behandling av personopplysninger**

3.1 Rettslig grunnlag for behandling av personopplysninger

a) Den registrerte har **samtykket** til behandling av sine personopplysninger for ett eller flere   
 spesifikke formål. *Legg ved kopi av samtykkeerklæring og informasjonsskriv.*

Behandlingen er **nødvendig** for:

b) å oppfylle en **avtale** som den registrerte er part i,

c) å oppfylle en **rettslig forpliktelse** som påhviler UiO som behandlingsansvarlig,

d) å verne den registrertes eller en annen fysisk persons **vitale interesser**,

e) å utføre en oppgave i **allmennhetens interesse** eller utøve offentlig myndighet som   
 UiO er pålagt,

f) formål knyttet til de **berettigede interessene** som forfølges av UiO eller en tredjepart,  
 med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går  
 foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.

Dersom behandlingsgrunnlaget er c) eller e), må supplerende lovhjemmel vises til:

3.2 Rettslig grunnlag for behandling av særlige kategorier av personopplysninger

Behandler ingen særlige kategorier av personopplysninger

Gjelder behandlingen særlige kategorier av personopplysninger, jf. punkt 2.4, må det i tillegg angis om behandling av slike opplysninger er omfattet av unntakene i personvernforordningen artikkel 9 nr. 2.

Den registrerte har gitt **uttrykkelig samtykke** til behandlingen av særlige kategorier av   
 personopplysninger. *Legg ved kopi av samtykkeerklæring og informasjonsskriv.*

Behandlingen er nødvendig for at UiO eller den registrerte skal kunne oppfylle sine forpliktelser  
 og utøve sine særlige rettigheter på området **arbeidsrett**.

Behandlingen gjelder personopplysninger som det er åpenbart at den registrerte har **offentlig-  
 gjort**.

Behandlingen er nødvendig av hensyn til viktige **allmenne interesser** på grunnlag av nasjonal rett

Behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til   
 vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med art. 89 nr. 1.

3.3 Formålsbegrensning og dataminimering

Formålet med behandlingen er oppgitt i punkt 2.1. Personopplysningene som behandles skal være adekvate, relevante, nødvendige og begrenset til det som er nødvendig for å oppnå formålene (prinsippet om dataminimering).

Følgende tiltak planlegges for å sikre dataminimering: De som ønsker å benytte seg av tilbudet på studentklinikken, sender en elektronisk søknad. Klinikken ønsker å motta søknader via søknadskjema, ikke via e-post, for å unngå at sensitive opplysninger sendes på e-post og at kun opplysninger vi spør om blir oppgitt. I søknaden bes det om å beskrive hva som ønskes hjelp til (vansker eller diagnoser). Det kreves å oppgi telefonnummer og postadresse. For å minimere persondata i journalsystemet vil studentene og veiledere få innføring pasientjournalloven slik at reglene og retningslinjene overholdes.

3.4 Lagring

Lagringstid skal beskrives og begrunnes. Det må tas stilling til hvor lenge det vil være behov for behandling av personopplysningene:

Forhåndsfastsatte slettedatoer (spesifiser og begrunn med tid for behandling, etterfølgende  
 oppbevaring for dokumentasjon/arkivformål).

Tidsbegrenset, men uten fastsatt dato (angi kriterier for fastsetting av varighet)

*Her må det fastsettes en foreløpig slettedato eller dato for ny vurdering av behov for videre   
 oppbevaring.*

Spesifiser lagringstid og dato for sletting/anonymisering: Etter pasientjournalloven § 25 skal helseopplysninger i pasientjournal oppbevares til det ikke lenger antas å være bruk for dem. Hvis ikke opplysningene deretter skal bevares etter arkivloven eller annen lovgivning, skal de slettes. Dato for ny vurdering av behov for videre oppbevaring: 10 år fra oppføringenes dato.

3.5 De registrertes rettigheter

3.5.1 Informasjon om behandlingen

Det må beskrives hvordan informasjon om behandling av personopplysninger vil gis til de registrerte. Informasjonsplikten gjelder for alle administrative behandlinger.

Beskriv hvordan de registrerte blir informert om behandlingen av deres personopplysninger:

Informasjon gis på klinikkens hjemmeside, og i klientenes samtykkeskjema.

3.5.2 Rett til innsyn, behandlingsbegrensning, retting, sletting og dataportabilitet.

Rett til innsyn, behandlingsbegrensning, retting, sletting og dataportabilitet gis til klinikk-klienter i henhold til gjeldene lover. Dette informeres om i klientenes samtykkeskjema og på klinikkens hjemmeside.

**Del IV. Personvern, risikoanalyse og tiltak**

Vurdering av risiko for de registrertes rettigheter og friheter, og planlagte tiltak for å håndtere risikoene. Kun risiko og konsekvens for den registreete skal vurderes, og ikke risiko og konsekvens for UiO/virksomheten.

4.1 Risiko for den registrerte

Vurdering av risikoens opprinnelse, art, særegenhet og alvorlighetsgrad. Vurderingen skal gjøres fra de registrertes perspektiv for hver risiko:

* Manglende reell medbestemmelse
* Manglende reell åpenhet
* Manglende forutsigbarhet
* Risiko for den registrerte hvis opplysninger kommer på avveie
* Bortfall eller svekkelse av andre rettigheter etter andre lover (for eksempel studierett, klagerett, ytringsfrihet, trygderett, religionsfrihet, rett til godt arbeidsmiljø).

Avklar potensielle konsekvenser, anslå alvorlighetsgrad, identifiser trusler og anslå sannsynlighet.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hendelse** | **Konsekvenser** | **Alvorlighetsgrad** | **Trusler** | **Sannsynlighet** |
| Manglende reell medbestemmelse – innsyn og endring av journal. | Klienter skal ha fullstendig og enkel mulighet til innsyn i sin journal, og andre lagrede opplysninger. Klienter har rettigheter til å kreve endring, tillegg og sletting av sine opplysninger. Konsekvensen hvis dette ikke overholdes er at klinikken begår lovbrudd, at det er feilaktig informasjon i systemet, og at klienten føler seg krenket. | Høy | At klienten ikke får korrekt informasjon ang. sine rettigheter, herunder at klinikkens web-sider og/eller samtykkeskjema ikke er tydelige nok, eller at klinikkens medarbeidere ikke er informert om forholdene eller er utydelige i sin kommunikasjon. I tillegg er det viktig å legge til rette for enkel tilgang og endring av journaler. | Lav. Informasjon om rettigheter blir gitt på nettsider, og til alle klinikkmedarbeidere ved oppstart. Klinikkens journalsystem er også enkelt å bruke, og det er enkelt å endre tidligere oppføringer, inkludert sletting. |
| Manglende reell åpenhet – innsyn i journal og journalsystemets tekniske drift. | Se punkt ang. medbestemmelse ovenfor. I tillegg kommer klientenes rettigheter til å vite hvordan journalsystemet opererer teknisk sett. Brudd på denne rettigheten kan medføre at klinikken begår lovbrudd. | Høy | Manglende informasjon på klinikkens nettsider, og på klientenes samtykkeskjema. | Lav. Informasjon blir gitt på nettsidene og på klientenes samtykkeskjema. |
| Manglende forutsigbarhet | Brukerne skal ha gode og tydelige muligheter til å melde fra om sine behov, som inkluderer klager, spørsmål, avtaler, avmelding, og interesse-påmelding. Konsekvens av manglende systemer for dette kan være at klinikken begår lovbrudd. | Høy | Manglende informasjon på klinikkens nettsider, og på klientenes samtykkeskjema. | Lav. Informasjon blir gitt på nettsidene og på klientenes samtykkeskjema. Nettsiden har tydelige knapper og lenker der man kan sende inn klager, trekke seg, stille spørsmål, og lignende. |
| Risiko for klientene hvis opplysninger kommer på avveie | Kan medføre alvorlige konsekvenser for klientene, siden opplysningene vi samler inn kan være av høyst personlig karakter. Slike hendelser kan være lovbrudd. | Høy | a) Data-angrep (hacking) på journalsystemet.  b) Sensitive opplysninger nedføres utenfor journalsystemet.  c) Svikt i tilgangskontrollen på klientenes opplysninger. | a) Lav. Klinikken bruker TSD til lagring og behandling av journal og andre opplysninger. TSD er spesifikt opprettet for å kunne håndtere lagring av sensitive opplysninger.  b) Lav. Følgende tiltak gjennomføres for å redusere risiko: 1) Alle opplysninger skal i utgangspunktet føres direkte inn i TSD, uten mellomledd. Dvs. at klinikkens medarbeidere må være innlogget i TSD for enhver nedføring av sensitive opplysninger. Ved bruk av papir for arbeidsnotater og test-resultater skal dette i utgangspunktet være avidentifisert og lagres kun i låsbare arkivskap i klinikkens lokaler. 2) Lyd og video-opptak må nødvendigvis gjennomføres med mellomlagring av data utenfor TSD. Klinikken har klare rutiner for håndtering av dette, blant annet dedikert utstyr i egne undersøkelsesrom, med krypterte lagringsdisker, og rutiner for umiddelbar overføring av data til TSD. 3) Klinikkens medarbeidere blir skriftlig informert bl.a. gjennom samtykkeskjema om alvorligheten av sensitive opplysninger på avveie, og at lovbrudd kan føre til straffeforfølgelse.  4) Klinikkens medarbeidere blir skriftlig informert om rutiner for behandling av ikke-sensitive opplysninger utenfor TSD.  c) Lav. Klinikken bruker TSDs løsninger på tilgangsstyring, slik at hver enkelt klinikk-medarbeider kun har tilgang til de elektroniske mappene tilknyttet spesifikke klinikk-klienter. Tilgang til mappe opprettes kun når klinikk-medarbeiderens faglige veileder via eget nettskjema har meldt inn tilknytning mellom klinikk-medarbeider og klinikk-klient. Dette nettskjema spesifiserer også når tilgangen gjelder fra/til. |
| Bortfall eller svekkelse av andre rettigheter etter andre lover (for eksempel studierett, klagerett, ytringsfrihet, trygderett, religionsfrihet, rett til godt arbeidsmiljø). | Medfører alvorlige konsekvenser. | Høy | Ingen | Lav |
| Opplysninger som feilaktig er endret eller slettet ikke kan gjenopprettes med minst en måneds historikk. | Kan medføre brudd på journalloven og/eller andre lover. | Høy | Feilaktig sletting/endring gjøres mellom to backup-sykluser. | Lav. Det er to automatiske backup-rutiner i TSD. Det ene utfører backup hver natt, og lagrer dette i opp til 7 dager. Det andre tar backup 2-3 ganger i uken, og lagrer dette i 90 dager. Hvis data blir opprettet og deretter endret/slettet mellom backup-sykluser, dvs. i løpet av hhv. 1 (system 1) eller 2-3 (system 2) dager, er det fare for at original dataene ikke kan gjenopprettes. Dette gjelder altså kun data som ble nedført de siste 3 dager (system 2), eller den siste dagen (system 1) hvis man oppdager hendelsen innen 7 dager. I slike tilfeller burde det være mulig for den journal-ansvarlige å huske de viktigste opplysningene i nedføringen, slik at disse kan nedføres på nytt. I tillegg er det normalt kun veileder, student, og klinikkens administrator som har tilgang til journaldata, slik at sannsynligheten for feilaktig sletting/endring reduseres ytterligere. |

4.2 Tiltak

Spesifiser tiltak for å håndtere risikoene for de registrerte og andre berørte personers rettigheter og friheter.

* Spesifikke garantier for å minimere inngripen
* Spesifikke sikkerhetstiltak som angår personopplysninger som skal behandles
* Generelle sikkerhetstiltak som iverksettes på systemet hvor behandlingen utføres
* Organisatoriske tiltak (styring)

Søknad om behandling sendes til Oslo SPeLL klinikken via nettskjema med direkte kobling til Tjenester for Sensitive Data (TSD). Evt. oversendelse av persondata fra andre institusjoner gjøres også via TSD-nettskjema. TSD har høyeste grad av sikkerhet for å beskytte særlige personsensitive data. TSD brukes også til klinikkens annen lagring og journalføring. I de tilfellene notater og andre midlertidige lagringsmedia (e.g. minnekort) benyttes skal det kun foregå på klinikkens lokaler, og de skal oppbevares i låsbare arkivskap. Alle studenter og veiledere ved klinikken må underskrive samtykkeskjema om at de har satt seg inn i klinikkens regler og følger disse.

Det stilles krav om at klienten samtykker til testing og behandling. Klienten skal ha adgang til opplysninger om egen situasjon og om den hjelpen som ytes. Klienten skal også informeres om mulige risikoer og bivirkninger. Klienten skal opplyses om at tjenesten skal ytes av en student, hvem som er studentens veileder, hva slags veiledning som vil bli gitt, veileders rolle i behandlingen og informasjon om at behandlingstimer kan bli diskutert med veileder/andre veiledere eller sammen med andre studenter dersom dette er aktuelt. Informasjon er videre avgjørende for at klienten kan medvirke og samtykke til tjenesteytingen.

Alle ansatte, studenter og veiledere ved Oslo SPeLL klinikken har plikt til å være kjent med gjeldende taushetspliktbestemmelser. Veiledere, studentene og ansatte underskriver en særskilt taushetserklæring. Etter Helsepersonelloven § 25 kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp og om pasienten ikke motsetter seg det.

Klienten informeres også at han har rett til å klage på den helse- og omsorgstjeneste han eller hun har mottatt ved utdanningsinstitusjoners studentklinikk.

Hvis klienten har kommentarer eller ønsker å klage på tjenesten, kan dette skjema brukes [Klageskjema](https://nettskjema.no/a/154606).

4.3 Samlet vurdering av personvernet

Gjør en oppsummering av personvernet og personopplysningssikkerheten i systemet/tjenesten.

Dette prosjektet har potensielt store utfordringer med hensyn til personvernet og personopplysningssikkerheten. Hovedutfordringen kommer av det samles inn sammenfattede person- og helseopplysninger, og spesielt fordi opplysningene kan komme fra barn. For å ivareta personvernet og personopplysningssikkerheten legger klinikkens databehandlingssystemer til rette for at:

1. Gjeldende lovverk og retningslinjer kan overholdes.
2. Alle parter informeres tilstrekkelig om lover og retningslinjer gjennom samtykkeskjema og informasjonsskriv.
3. Det utøves individuell styring tilganger til personopplysninger, med klart definerte rutiner ved tilgangsklarering.
4. Personopplysninger oppbevares og behandles slik at datasikkerheten kan ivaretas.

Klinikkens systemer vurderes derfor å tilfredsstille ivaretakelse av personvernet og personopplysningssikkerheten.

**Del V. Involvering og drøftelser**

5.1 De registrerte

Som utgangspunkt skal man innhente synspunkter på behandlingen fra de registrerte eller representanter fort de registrerte når det er relevant.

Synspunkter er innhentet:

Ja

Nei

Begrunnelse: Etter pasient- og brukerrettighetsloven har klienten rett til å medvirke ved gjennomføring av hjelpen som tilbys. Klienten har rett til å medvirke ved valg mellom tilgjengelige og forsvarlige undersøkelses- og behandlingsmetoder.

5.2 Personvernombud

Personvernombudet skal på anmodning involveres ved utarbeidelsen av personvernkonsekvensvurderinger, og synspunkter innarbeides.

5.3 Forhåndsdrøfting med Datatilsynet

Skal Datatilsynet kontaktes for forhåndsdrøfting i tråd med personvernforordningen artikkel 36? Dette er aktuelt når den administrative behandlingen innebærer høy risiko for personvernet, og denne risikoen ikke lar seg minimere av de kartlagte tiltak i punkt 4.2.

*Dette punktet skal drøftes med personvernombudet.*

Konklusjon:

5.4 Plan for implementering av tiltak

De tiltak som er identifisert som hensiktsmessige for oppfølging av denne personvernkonsekvensvurderingen er følgende: [Oppsummering av supplerende risikoreduserende tiltak fra risikoregisteret og tiltak fra eventuelt andre kapitler.]

For å ivareta personopplysningssikkerheten i den administrative behandlingen, vil følgende tiltak iverksettes:

|  |  |  |
| --- | --- | --- |
| Tiltak | Tidsfrist | Ansvar |
| Ferdigstille nettside med kvalitetshåndboken for studentklinikken på ISP | [] 2020 | Anders Lunde, Vasiliki Diamanti |
| Ferdigstille TSD-nettskjema og TSD journalsystem | [] 2020 | Anders Lunde |
| Ferdigstille retningslinjer for bruk av TSD journalsystem for studenter og veiledere | [] 2020 | Anders Lunde, Vasiliki Diamanti |
| Ferdigstille informasjons- og samtykkeskriv (for personer som ønsker behandling). | [] 2020 | Anders Lunde, Vasiliki Diamanti |
| Integrere elektronisk samtykke i TSD-nettskjema | [] 2020 | Anders Lunde |

**Del VI. Godkjenning**

|  |  |  |
| --- | --- | --- |
| Dato | Versjon av DPIA | Godkjent av |
|  |  |  |
|  |  |  |

**Del VII. Vedlegg**

|  |
| --- |
| **7.1. Informasjon til klient og samtykkeskjema i forbindelse med bruk av klientopplysninger i undervisning ved Oslo SPeLL studentklinikk ved Institutt for spesialpedagogikk**  **Bakgrunn**  Oslo SPeLL studentklinikken ved Institutt for spesialpedagogikk tilbyr helsehjelp til barn som har spesielle pedagogiske behov, så vel som voksne som har fått kommunikasjonsvansker, vanligvis som et resultat av hjerneslag eller hjerneskade.  Tjenestene klinikken tilbyr inkluderer vurdering/testing av klienter for å identifisere vanskelighetsområder og korte programmer for utbedring/terapi hvor studentene jobber under nøye tilsyn av en klinikker.  **Bruk av klientopplysninger i forbindelse med veiledning og undervisning**  Klientopplysninger vil journalføres og lagres i henhold til gjeldende regelverk for pasientjournaler og helsepersonell. Tilgang til din journal er begrenset til dine behandlere hos oss.  Materiale fra vurdering og terapiprogrammer drøftes med veileder. Formålet er å gi deg best mulig utbedring, samt gi studentene god opplæring i klientbehandling.  All undervisning i vår klinikk legger vekt på ivaretagelse av din personlige integritet og verdighet. Studenter og veiledere har taushetsplikt om personlige forhold de får kjennskap til i behandlingen og undervisningen. Alle som deltar i veiledningen og undervisningen har taushetsplikt og har undertegnet egen taushetserklæring. |

**Hva skjer med informasjonen om deg?**

Etter pasientjournalloven § 25 skal dine helseopplysninger i pasientjournal oppbevares til det ikke lenger antas å være bruk for dem.

Testresultater, videoopptak og andre opplysninger lagres i Tjenester for Sensitive Data (TSD). TSD er en datatjeneste ved Universitetet i Oslo med høyeste grad av sikkerhet for å beskytte særlige personsensitive data. Alle personopplysninger vil bli behandlet konfidensielt. UiO er ansvarlig for oppbevaring og disponering av test resultater og video opptakene. Arbeidsnotater fra forsamtaler og notater fra terapitimer skal oppbevares i låsbart arkivskap til de skannes i TSD systemet. Dette må skje ikke senere enn 1 dag etter samtale. Materialet skal være avidentifisert, dvs. at det ikke skal inneholde direkte personidentifiserbare opplysninger.

Klinikkens medarbeidere blir skriftlig informert bl.a. gjennom samtykkeskjema om alvorligheten av sensitive opplysninger på avveie, og at lovbrudd kan føre til straffeforfølgelse.

**Samtykke**

Det er en forutsetning for å motta behandling ved vår studentklinikk at du samtykker til at vi kan bruke opplysninger fra behandlingen i veiledning og undervisning.

Du kan når som helst trekke tilbake samtykket, men da vil behandlingen måtte avsluttes. Tilbaketrekking av samtykket vil ikke ha konsekvenser for ditt fremtidige forhold til Institutt for spesialpedagogikk. Retten til å trekke tilbake samtykke vil gjelde for alle som deltar, også familiemedlemmer eller andre pårørende.

**Rett til innsyn og medvirkning**

Du har rett til innsyn i opplysninger som er lagret om deg.

Du har rett til å medvirke ved gjennomføring av hjelpen som tilbys og ved valg mellom tilgjengelige og forsvarlige undersøkelses- og behandlingsmetoder.

**Rett til å klage**

Du kan sende en klage hvis du synes du ikke får den helsehjelp, informasjon og annen bistand du har krav på. Klagen sendes inn via dette skjemaet: [Klageskjema](https://nettskjema.no/a/154606)

Alle klager blir behandlet og besvart av leder for studentklinikken. Dersom du ønsker det kan klagen sendes videre til Fylkesmannen.

|  |  |
| --- | --- |
| **Skjema for samtykke til bruk av klientopplysninger i forbindelse med veiledning/undervisning ved Oslo SPeLL studentklinikken ved Institutt for spesialpedagogikk UiO** | |
| Oslo SPeLL (Oslo SpesialPedagogikk- og LæringsLab)  Institutt for spesialpedagogikk, Universitetet i Oslo  Sem Sælands vei 7, 0317 Oslo  Telefonnummer til ekspedisjonen: 22 85 80 59 | |
| Jeg samtykker til at opplysninger fra min behandling kan brukes i veiledning og undervisning som beskrevet i dette informasjonsbrevet.  Har du spørsmål om bruken av dine opplysninger, kan du kontakte Oslo SPeLL studentklinikk på telefon: 22856072 | |
| Navn med blokkbokstaver | |
| Dato | Underskrift |

**Retningslinjer for bruk av TSD journalsystemet (student)**

Som student på emnet \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ skal du bruke TSD journalsystemet som en del av opplæringen.

**Klientinformasjon**

* All klientinformasjon er konfidensiell og taushetsbelagt.
* Klientinformasjon er sensitiv informasjon og skal håndteres etter gjeldene regler.

Bruk av systemet

* Bruk av tjenesten for sensitive data (TSD) skal kun gjøres ifra henviste dedikerte arbeidsstasjoner på Oslo SPeLL klinikken i Sem Sælands vei 7.
* Arbeidsstasjonene skal kun benyttes til angitt formål, dvs. digital journalføring ved bruk av TSD.
* Uautorisert endring og/eller plassering av arbeidsstasjonen er ikke tillatt.
* All eksport og utskrift av data fra systemet skal kun gjøres av autorisert personell, på Oslo SPeLL klinikken i Helga Engs hus i Sem Sælands vei 7.
* Systemet skal kun benyttes som anvist, all uautorisert endringen av system og/eller klientinformasjon vil betraktes som brudd på reglementet.
* Aldri forlat arbeidsstasjonen med innlogget sesjon i systemet. Ved kortere pauser påse at arbeidsstasjonen låses eller logg ut sesjonen ifra systemet.

Brudd på reglementet

Ved å signere på dette dokumentet forplikter du deg til å følge reglementet over. Brudd på avtalen som innebærer overtredelser av f.eks. personopplysningsloven, helsepersonelloven og/eller universitets- og høyskoleloven, kan medføre sanksjoner i form av utestenging fra studiet i inntil 3 år (uhl. § 4-8 annet ledd), tilbakekalling av autorisasjon etter helsepersonelloven, straff, tvangsmulkt og/eller overtredelsesgebyr.

Oslo (dato):

Studentens signatur:

Studentens navn med blokkbokstaver:

Studentnummer:

**{Retningslinjer for bruk av TSD journalsystemet (veileder)}**

**Retningslinjer for bruk av TSD journalsystemet (veileder)**

Som veileder på emnet \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ skal du bruke Tjeneste for sensitive data (TSD) journalsystemet som en del av opplæringen.

Klientinformasjon

* All klientinformasjon er konfidensiell og taushetsbelagt.
* Klientinformasjon er sensitiv informasjon og skal håndteres etter gjeldene regler.

Bruk av systemet

* Bruk av TSD tjenesten kan gjøres ifra henviste dedikerte arbeidsstasjoner på Oslo SPeLL klinikken i Sem Sælands vei 7.
* Arbeidsstasjonene skal kun benyttes til angitt formål, dvs. digital journalføring ved bruk av TSD systemet.
* Veiledere har mulighet til å logge seg på TSD via ID-portal i skjermede omgivelser utenfor klinikken.
* Systemet skal kun benyttes som anvist, all uautorisert endringen av system og/eller klientinformasjon vil betraktes som brudd på reglementet.
* Aldri forlat arbeidsstasjonen med innlogget sesjon i systemet. Ved kortere pauser påse at arbeidsstasjonen låses eller logg ut sesjonen ifra systemet.
* Forsamtale med klienten skal foregå på Oslo SPeLL sine lokaler.
* Samtykke fra pasient skal skannes inn etter forsamtale, eller senest etter første samtale med student.
* Alle klienter skal ha forsamtalenotat.
* Notat fra forsamtale skal skrives direkte i TSD systemet.

Oslo (dato):

Veileders navn og signatur: