Referanse 2013/994 Bergen 12/3 2014

Rapport fra arbeidsgruppe for sikker lagring av og tilgang til forskningsdata ved UiB

Sammendrag og anbefalinger

Utvalget har vurdert løsninger for oppbevaring og behandling av forskningsdata ved UiB og har identifisert konkrete tiltak som vil styrke sikkerhet og brukervennlighet for forskningen ved institusjonen. Utvalget har forholdt seg til gjeldende normer for datasikkerhet og behovet for sikre fremtidsrettede løsninger for forskningsmiljøene. Vi ser det som avgjørende at forskere opplever løsningene som en forbedring av arbeidssituasjonen slik at systemet ikke virker uhensiktsmessig og hemmende. Implementering av tiltakene vil trenge noe tid til utprøving og opplæring, og vil få noen budsjettmessige konsekvenser. UiB bør sette klar tidsfrist for dette arbeidet.

Utvalget foreslår følgende tiltak:

1) Det utvikles en egen forskningsserverløsning med to-faktor autentisering av brukerne for prosjekter som i hovedsak er UiB-interne og som behandler sensitive persondata
   a) IT-systemet bør oppfylle kravene i «Norm for informasjonssikkerhet» (se side 5)
   b) Forskningsserveren må ha regnekraft og programvare som kan dekke de fleste behov for behandling av forskningsdata
   c) Forskningsserveren må administreres slik at uvedkommende ikke får tilgang og at data ikke kommer på avveie
   d) Forskere må sikres enkel oppkobling fra klientdriftet maskin ved UiB eller tilsvarende fra samarbeidende institusjoner via vanlig internettforbindelse
   e) Pilotprosjekter som tester serverløsningen bør gjennomføres ved enkelte institutter eller fakulteter snarest
2) Det stilles strenge krav til behandling av sensitive persondata utenfor en sikker forskningsserverløsning for ansatte og studenter ved UiB
   a) Når forsker er i tvil skal en sikker server-løsning brukes
   b) Sensitive data kan kun oppbevares kryptert utenfor serveren
   c) Data bør overføres direkte fra dataleverandør til forskningsserver
   d) Annen nasjonal infrastruktur med høy grad av sikkerhet, for eksempel TSD-systemet ved UiO, kan brukes av større nasjonale og internasjonale samarbeidsprosjekter

    e) Forskere med tilgang til helsenettet skal kunne bruke den tilsvarende serverløsningen som tilbys av Helse Vest-IKT
3) Det utvikles en avtale- og akkrediteringsordning og praktiske løsninger for eksterne forskere som skal ha tilgang
4) Det innføres en egenmelding hvor forskere redegjør for hvilke data de har tilgang til
    a) Ordning med egenmelding prøves ut ved noen institutter
    b) Egenmelding innhentes rutinemessig med jevne mellomrom
5) Ordningen med egenmelding administreres av institutt eller fakultet i samarbeid med forskningsavdelingen som en del av UiB's internkontrollsystem for forskningsprosjekter.
6) Det utvikles et system med instituttvise eller fakultetsvise prosjektoversikter og registrering av avviksmeldinger som del av UiB´s internkontrollsystem
7) Det utvikles dokumentasjon og prosedyrer for sikker databehandling
8) Det lages en kommunikasjons- og opplæringsplan
9) Implementeringen får en klar tidsplan

1. Bakgrunn og gruppens arbeid

Arbeidsgruppe for sikker lagring av og tilgang til forskningsdata ved UiB ble oppnevnt av rektor 08.02.2013 (ePhorte 2013/994). Det vises til sak 53/12 i universitetsstyret om universitetets implementering av lov om medisinsk og helsefaglig forskning i forbindelse med revisjon av universitetets internkontrollsystem for behandling av personopplysninger i forskningsprosjekter. Videre vises det til diskusjoner i møte 5.11.12 mellom prorektor og representanter for fakultetene om lagring av forskningsdata ved UiB og senere kontakt med fakultetene og IT-avdelingen. Det stilles spørsmål ved om forskningsdata er godt nok sikret, hvordan det tilrettelegges for sikker lagring av forskningsdata og hvordan rutinene for lagring følges opp og utvikles. Hvordan forskere informeres om hvilke regler og rutiner som gjelder for lagring av data ble også tatt opp. Det var ønskelig at en arbeidsgruppe kunne komme med anbefalinger for ytterligere tiltak.

Viktig bakgrunn for arbeidet finnes i rapporten fra «Rokne-gruppen» av 16/12 2011: «Implementering av helseforskningsloven og revisjon av internkontrollsystemet for behandling av personopplysninger ved Universitet i Bergen».

Gruppens sammensetning var i utgangspunktet -

- Professor Rolv Terje Lie, Institutt for global helse og samfunnsmedisin, Det medisinsk-odontologiske fakultet, leder av gruppen
- Professor Pinar Heggernes, Institutt for informatikk, Det matematisk-naturvitenskapelige fakultet
- Professor Simon Øverland, HEMIL-senteret, Det psykologiske fakultet
- Førsteamanuensis Bjørn Henning Østenstad, Det juridiske fakultet
- Professor Ann Nilsen, Sosiologisk institutt, Det samfunnsvitenskapelige fakultet
- Professor Koenraad de Smedt, LLE, Det humanistiske fakultet
- Avdelingsdirektør Thomas Evensen, IT- avdelingen
- Avdelingsdirektør Svenn-Åge Dahl, Forskningsadministrativ avdeling

Svenn-Åge Dahl og Thomas Evensen har senere fratrådt sine stillinger og blitt erstattet av henholdsvis Heidi A. Espedal og Sidsel Storebø.

Gruppens mandat omfattet å

- Utrede og anbefale løsninger for sikker lagring av og tilgang til data
- Anbefale tiltak for å forbedre lagrings- og tilgangssituasjon
- Gi anbefaling om konkrete rutiner og prosedyrer (som for eksempel autorisasjoner, logging og selvangivelser) for lagring og tilgang av data og vedlikehold av datasystemer
- Gi anbefaling om sikkerhetsnivåer i datasystemene og foreslå systemmessige tiltak som støtter opp under rutiner, prosedyrer og sikkerhetsnivåer for datalagring
- Beskrive ansvarsforhold og institusjonell kontroll i et system for sikker behandling av og tilgang til data
- Gi anbefaling om igangsetting av pilotprosjekter
- Gi anbefaling om oppærings- og informasjonstiltak
- Gi anbefaling om hvordan systemer for sikker lagring og tilgang skal forvaltes slik at systemene både blir sikre og brukervennlige

Mange miljøer ved UiB, særlig ved HF og UB, har en rekke utfordringer når det gjelder sikring, lagring og deling av informasjon. Gruppen har imidlertid oppfattet og avgrenset mandatet til å gjelde behandling av sensitive persondata, og i mindre grad laging og tilgang for andre typer informasjon.

Et viktig premiss for arbeidet har vært å oppfylle Helsedirektoratet sine krav til datasikkerhet som er beskrevet i «Norm for informasjonssikkerhet» i helse- omsorgs- og sosialsektoren (se side 5). Selv om UiB som institusjon ikke er forpliktet til å følge denne normen i alle sammenhenger, mener gruppen at det er fornuftig å stille de samme kravene til et system for sikker databehandling ved UiB. UiB er kjent med og er underlagt normen i noen sammenhenger. Et eksempel er IT-systemet for odontologisk klinikk, som UiB drifter og som er underlagt kravene i Normen.

Arbeidsgruppen fikk opprinnelig frist til juni 2013, men på grunn av sen oppstart og utskifting i gruppen ble fristen forlenget uten nærmere angivelse av frist. Gruppen har avventet en risiko og sikkerhetsanalyse (ROS-analyse) av et pilotsystem for sikker databehandling (LSP) som har vært testet ut ved Institutt for global helse og samfunnsmedisin (IGS). ROS-analysen baserer seg på «Norm for informasjonssikkerhet». Gruppen har valgt å benytte dette som bakgrunn for noen av forslagene. Arbeidsgruppen har hatt 5 møter i perioden mai til oktober 2013 og har delt på skrivearbeidet.

2. Lovgivningens krav til behandling av sensitive persondata

Utvalget har avgrenset mandatet til å gjelde behandling av sensitive persondata. Begrepet «sensitive personopplysninger» er i personopplysningsloven (lov 14. april 2000 nr. 31) § 2 nr. 8 definert som opplysninger om

a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,

b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,

c) helseforhold,

d) seksuelle forhold,

e) medlemskap i fagforeninger.

Etter bokstav c) er altså opplysninger om «helseforhold» alltid sensitive. Ut fra volumet av helseforskning ved UiB har særlig sikkerhet for denne typen data blitt et startpunkt for utvalget sine vurderinger.

Helseforskningsloven (lov 20. juni 2008 nr. 44) § 6 regulerer hovedkrav til organisering av forskning, og lyder:

«Medisinsk og helsefaglig forskning skal organiseres med en forskningsansvarlig og en prosjektleder og beskrives i en forskningsprotokoll. Finansieringskilder må fremgå av protokollen.

Det skal føres internkontroll tilpasset virksomhetens størrelse, egenart, aktiviteter og risikoforhold.

Departementet kan gi forskrift med nærmere krav til organisering av medisinsk og helsefaglig forskning, krav til forskningsprotokollen og til internkontroll, samt gi bestemmelser om prosjektleders[3] og forskningsansvarliges plikter.»

Universitetet i Bergen vil være «forskningsansvarlig» når «det overordnede ansvaret for forskningsprosjektet» ligger ved institusjonen, jf. hfl. § 4 bokstav e. Kravene som da slår inn er utdypet i Forskrift om organisering av medisinsk og helsefaglig forskning (Forskrift 1. juli 2009, nr. 955). Fra § 3 hitsettes:

«Forskningsansvarlig har det overordnede ansvaret for forskningsprosjektet og skal minst sørge for

c) at forskningsdata […] behandles forsvarlig.»

Bestemmelsen omhandler den forskningsansvarliges plikter, og gjengir at den forskningsansvarlige har det overordnede ansvaret for forskningsprosjektet, jf. helseforskningsloven § 4 bokstav e. Det sentrale med hensyn til den forskningsansvarliges ansvar og plikter, er at denne har et organisatorisk ansvar på systemnivå.

Av bokstav c) fremgår at forskningsansvarlig skal sørge for at forskningsdata behandles *forsvarlig*. Forsvarlighet er altså et sentralt rettslig begrep, men som ikke har et entydig meningsinnhold. Begrepet «behandles» har samme innhold som «behandling» i personopplysningsloven § 2 nr. 2 og helseregisterloven § 2 nr. 5, det vil si at enhver bruk av forskningsdata omfattes, herunder innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter.

Personopplysningsloven og personopplysningsforskriften vil gjelde utfyllende for behandling av personopplysninger, jf. helseforskningsloven § 2 tredje ledd. I praksis betyr dette blant annet at det stilles krav til informasjonssikkerhet. Et sentralt element når det gjelder forsvarlig oppbevaring av forskningsdata, vil være ansvar for å sikre forsvarlige it-systemer og vedlikehold av disse.

Personopplysningsloven stiller blant annet krav om at det gjennom planlagte og systematiske tiltak skal sørges for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger, jf. § 13 første ledd. For å oppfylle kravet om informasjonssikkerhet må det iverksettes tiltak som skal

hindre at helseopplysninger fra prosjektet kommer uvedkommende i hende. I Veileder til helseforskningsloven heter det i punkt 2.5.2:

«Tiltakene bør minst vurderes ut i fra bruk av teknisk utstyr, tilgangsstyring, rutiner for avidentifisering og anonymisering av opplysninger og håndtering av avvik. Rutinene må også omfatte hva som skal skje med opplysningene ved avslutning av prosjektet.»

Kapittel 2 i Forskrift om behandling av personopplysninger (forskrift 15. desember 2000 nr. 1265) er noe mer dyptpløyende om informasjonssikkerheten. Her er nedfelt overordnede krav blant annet om at virksomheten selv skal «fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger» (§ 2-4), gjennomføre sikkerhetsrevisjon (§ 2-3) og avvikshåndtering (§ 2-4). Videre finner vi bestemmelser om ansvars- og myndighetsforhold for bruk av informasjonssystemet (§ 2-7), fysisk sikring av utstyr brukt i behandling av personopplysninger (§ 2-10), sikring av konfidensialitet (§ 2-11), overføring av personopplysninger til andre (2-15) og dokumentasjon av rutiner for bruk av informasjonssystemet (§ 2-16). Et overordnet synspunkt er at det gjelder et forholdsmessighetskrav (§ 2-1):

«de planlagte og systematiske tiltakene som treffes i medhold av forskriften, [skal] stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd».

I helse-, omsorgs- og sosialsektoren er det utarbeidet et dokument kalt «Norm for informasjonssikkerhet» (www.normen.no) som er ett av flere støttedokumenter for «Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren». Dokumentene er utarbeidet i samarbeid mellom representanter for offentlige myndigheter og berørte organisasjoner, og har dels karakter av en sammenfatning av relevant lov- og forskriftsverk, dels av enkelte presiseringer. Det er imidlertid også her tale om krav på et overordnet nivå. Normens punkt 4.4 omhandler nivå for akseptabel risiko. Dette må i den enkelte virksomhet fastsettes ut fra hensynet til konfidensialitet, tilgjengelighet, integritet og kvalitet.

Oppsummert kan vi slå fast at lovgivningen ikke stiller opp klare og konsise krav til informasjonssikkerhet ved forskningsdata. Det er derimot nedfelt noen mer overordnede krav og vurderingstema. Dette gir etter utvalgets vurdering UiB et visst skjønnsrom. I alle tilfeller må informasjonssikkerhet være noe man ved virksomheten har et gjennomtenkt forhold til. Krav om internkontroll framgår både av personopplysningsloven § 14 og helseforskningsloven § 4. Fra sistnevnte hitsettes:

«Med internkontroll menes systematiske tiltak som fremmer god forskning og som sikrer at forskningen planlegges, organiseres, gjennomføres og avsluttes i samsvar med krav fastsatt i eller i medhold av helseforskningsloven. Internkontroll skal dokumenteres og utformes i den form og det omfang som er nødvendig på bakgrunn av virksomhetens størrelse, egenart, aktiviteter og risikoforhold. Internkontroll skal ha styrende, gjennomførende og kontrollerende elementer, som innebærer at den forskningsansvarlige minst skal sørge for

a) at virksomhetens mål for forskningen, samt ansvars- og myndighetsforhold og hvordan forskningsvirksomheten strukturelt er tilrettelagt og organisert, er beskrevet
b) at det føres løpende oversikt over alle medisinske og helsefaglige forskningsprosjekter som involverer mennesker, humant biologisk materiale eller helseopplysinger innen eget ansvarsområde
c) å ha oversikt over de krav i og i medhold av helseforskningsloven og annet regelverk, som gjelder for

forskningen

d) at det utarbeides og dokumenteres rutiner som setter prosjektleder og medarbeiderne i virksomhetens forskningsprosjekter i stand til å overholde kravene som nevnt i bokstav c

e) at prosjektleder, medarbeidere og annet personell som er involvert i forskningsprosjekter har tilstrekkelig kompetanse

f) at det utarbeides og dokumenteres rutiner for å motta meldinger om avvik og sikre at avvik rettes

g) at det foretas systematisk overvåking og gjennomgang av internkontroll, for å sikre at den fungerer som forutsatt og bidrar til kontinuerlig forbedring i virksomheten.

Den forskningsansvarlige kan delegere oppgaver til andre, men ikke ansvar.»

I Forskrift om organisering av medisinsk og helsefaglig forskning av 1/7 2009 gjøres det klart at forskningsansvarlig skal sørge for at det tilrettelegges for at medisinsk og helsefaglig forskning blir utført på en måte som ivaretar informasjonssikkerhetsmessige forhold (§ 3). Prosjektleder har ansvar for at informasjonssikkerhetsmessige forhold ivaretas i den daglige driften (§ 5). I denne sammenhengen tolkes dette som at UiB har ansvar for å utvikle IT-systemer som gir god informasjonssikkerhet og at prosjektleder kun har ansvar for at disse brukes riktig i det daglige arbeidet.

3. Fagmiljøenes behov

Fagmiljøenes behov for sikker og god databehandling har økt i takt med det økende omfanget av forskning på store datasett fra kilder som nasjonale registre, biobanker, helseundersøkelser og kliniske forskningsprosjekter. Det er erkjent at datamengden og graden av detaljering, for eksempel knyttet til genetisk informasjon stiller store krav til sikker databehandling. Samfunnets krav til sikker databehandling og reell risiko knyttet til scenarier for datalekkasje og innbrudd har også økt. I tillegg er lover og regler for bruk og lagring av forskningsdata kompliserte. De sorterer under flere lovverk, og det kan være vanskelig for den enkelte forsker å vite eksakt hvordan data skal håndteres i et gitt tilfelle. Spørsmål om hva som i praksis er ”sensitive persondata” er heller ikke enkelt å bedømme i alle tilfeller. Slik usikkerhet gjør at mange forskere vil sette pris på et felles system som ivaretar hensynet til sikkerhet. Med dette som bakteppe, er vår oppfatning at de fleste forskere vil ønske velkommen et anerkjent og sikkert system for lagring og behandling av data.

For den enkelte forsker er det avgjørende at systemet er brukervennlig og gir tilgang til programmer og regneressurser. Eksempler på programvare som gruppen vet må være tilgjengelig er Nvivo, AMOS, MPLUS, R, SAS, SIGMAPLOT, SPSS og STATA. For flere av disse programmene vil det være svært viktig at forskerne får mulighet til å hente inn analysemoduler fra internett på en enkel måte. Det vil i praksis forutsette at IT-avdelingen kan bistå med slik innlasting og installering. Dersom systemet skal dekke alle behov for dataanalyse, vil listen av programmer som må kunne kjøres bli enda lengre og omfatte mer spesielle programmer. I et slikt scenario kan installering, oppdatering og vedlikehold by på kapasitetsutfordringer.

Systemet må kunne levere god regnekraft. For brukerne vil det være viktig at analyser ikke tar lengre tid enn på en egen ordinær maskin. Forskerne må oppleve et nytt og mer sikkert system som en forbedring, og hurtigere analyser vil bidra til dette. For prosjekter med særlig tunge behov, kan betaling for regnekraft vurderes.

Det er vanskelig å anslå omfanget av behovet for et IT-system for sikker behandling av sensitive data. Det finnes potensielle brukere ved de fleste fakulteter og et grovt anslag kan være at flere hundre forskere ved UiB vil ha behov for et slikt system. Det er viktig at systemet utvikles på en måte som gjør at det kan skaleres opp etter som behovene avdekkes og prosjekter fases inn.

Ved og rundt **Det matematisk-naturvitenskapelige fakultet** er det tre miljøer som driver med forskning som involverer lagring og behandling av sensitive personopplysninger: Institutt for biologi (BIO), Molekylærbiologisk institutt (MBI) og Computational Biology Unit (CBU) ved Uni Research. Når det gjelder forskere hos BIO og MBI, har disse enten selv en tilknytning til Helse Bergen og deres forsknings infrastruktur eller en samarbeidspartner på samme prosjekt som har slik tilknytning. Det vil si at sikkerheten rundt de sensitive data rutinemessig etableres i samarbeid med Helse Bergen. Det samme gjelder i stor grad også forskere ved CBU. I tillegg har CBU et samarbeid om infrastruktur med Medisinsk Genetikk ved Haukeland Universitets Sykehus, hvor CBU tilbyr sikrede servere for analyse av sekvenseringsdata, også humane prøver. Dette skjer på sikrede Unix servere med begrenset tilgang til få personer. For den mest kritiske serveren er CBU i dialog med Helse Bergen for å kvalitetssikre og få godkjent sikkerhetstiltakene og etablere direkte dataoverføring etter analyse til forskningsserveren på Helsenettet. Akkurat nå er CBU i gang med å starte opp som en nasjonal ELIXIR node og tilby sikker lagring av sensitiv data via sitt samarbeid med USIT ved UiO gjennom TSD. Dette skal i utgangspunktet gjøre det mulig for forskere tilknyttet CBU å kunne håndtere sensitiv data uten at de trenger tilgang til Helse Bergen sin infrastruktur for forskning.

Ved **Det medisinsk-odontologiske fakultet** foregår det meste av den pasientrettede forskningen i de sykehustilknyttede miljøene ved de kliniske instituttene (K1 og K2) innenfor forskningsserversystemet på Helsenettet som driftes av Helse Vest IKT. Som avtalt i 2010 utføres internkontrollen knyttet til denne aktiviteten nå av Helse Bergen HF. Ved Institutt for global helse og samfunnsmedisin behandles data fra helseregistre, biobanker, egne prosjekter og primærhelsetjenesten innenfor rammen av UiB sine IT-systemer. Prosjekter benytter i varierende grad tiltak som separate maskiner frikoblet fra internett og krypteringsrutiner avhengig av hva som er avtalt med REK eller Datatilsynet. Instituttet har i samarbeid med IT-avdelingen utviklet forskjellige systemer for sikker lagring og behandling av forskningsdata. Det ene systemet ligner på det som ble foreslått i Rokne-rapporten. Systemet er blitt vurdert til ikke å ha tilstrekkelig sikkerhet og brukervennlighet. Det andre systemet (LSP) har vært i drift en kort tid i sin nåværende form og er nylig blitt vurdert i en ROS-analyse opp mot kravene i Normen (www.normen.no). Systemet bør testes og videreutvikles og vil kunne danne et utgangspunkt for en fellesløsning slik den skisseres av dette utvalget. Det registerfaglige miljøet er sterkt knyttet til og samlokalisert med Avdeling for helseregistre ved Nasjonalt folkehelseinstitutt (FHI). Enkelte samarbeidsprosjekter gjennomføres innenfor FHI sitt IT-system og internkontrollsystem. Instituttet har omfattende nasjonalt og internasjonalt samarbeid som IT-løsningene også bør tilrettelegge for. Senter for internasjonal helse forvalter data fra en rekke forskningsprosjekter i lav- og mellominntektsland og har omfattende samarbeid med forskere i disse landene. IGS ser et behov for et sikrere, mer brukervennlig og mer standardisert IT-system for sikker databehandling og en styrket internkontroll på instituttnivå. Andre forskningsmiljøer ved fakultetet som ikke dekkes av helseforetaket sine løsninger vil ha lignende behov.

Ved **Det psykologiske fakultet** jobber flere forskere på prosjekt basert på kliniske data. Fakultetet besitter også egne journalsystemer for pasientbehandling. Andre av fakultets forskere arbeider med registerdata, survey- og intervjudata som kan inneholde personopplysninger, og også kvalitative data i form av lydopptak og video. Fakultetet har forskningsmiljø som leder store multinasjonale undersøkelser. En rekke prosjekter foregår i samarbeid med andre institusjoner, og forskere og stipendiater innen UiB-prosjekt kan ha daglig arbeidssted ved andre institusjoner. Det psykologiske fakultet har dermed stor diversitet når det gjelder bruk av ulike datatyper i forskning (og undervisning), og må forholde seg til regelverk for både helseforskning og data med andre typer personopplysninger. Forskerne ved fakultetet har behov for trygghet i databehandlingen, og fakultetet har et behov for oversikt og kontroll med databehandlingen som skjer ¬ både i «helseforskningslinjen» via REK og i «persondatalinjen» via NSD/Personvernombudet. Et felles, oversiktlig og brukervennlig system som også ivaretar hensyn til sikker databehandling vil være til betydelig nytte for forskningen ved det psykologiske fakultet.

Ved **Det samfunnsvitenskapelige fakultet** har man siden tidlig på 1990-tallet arbeidet med avidentifiserte fullpopulasjons individdata fra administrative registre. Opplysningene er delvis sensitive (helseopplysninger inkludert diagnose, trygde- og arbeidsmarkedssituasjon, familieforhold, etnisitet, osv.), og er blitt utlevert etter konsesjoner fra dataeiere (NAV, SSB m.fl.) og Datatilsynet. Gruppe for trygdeøkonomi har stått for en relativt stor og vedvarende analyseaktivitet i denne perioden, men har hatt utstrakt samarbeid med kollegaer på og utenfor fakultetet (f.eks. Sosiologisk institutt, Institutt for global helse og samfunnsmedisin og Rokkansenteret). Gruppen tok på eget initiativ i 2010 kontakt med IT-avdelingen og fikk i stand et opplegg for sikker databehandling som fremdeles er aktivt: 1) De sensitive dataene ble overført til server driftet av IT-avdelingen. 2) Data fra denne serveren deles ut gjennom brannmur til klienter som er godkjent av prosjektleder. 3) Data kan brukes fra vanlige Windows- og linuxklienter, og innlogging er begrenset til kun definerte brukere, og kun fra UiB-nett/VPN. Selv om systemet representerte et stort fremskritt når det gjelder kontroll og oversikt, kan det ytterligere forbedres når det gjelder sikkerhet. Videre har tyngre analysejobber fra arbeidsplass utenfor campus i praksis vært umulig på grunn av reduksjonen i hastighet som skjer ved pålogging via VPN. Gruppe for trygdeøkonomi er derfor i disse dager i ferd med å implementere den nye LSP-løsningen som er beskrevet annet sted i denne rapporten. Gruppen har selv finansiert deler av dette ved innkjøp av server og programvare (Stata) og er i ferd med å prøve ut det nye systemet. Det er for tidlig å konkludere med hensyn til brukervennlighet. Det er et ønske fra miljøet at slusefunksjonen som gjør det mulig å importere og eksportere for eksempel tabeller, figurer og kommandofiler til programmer må kunne brukes uten for mange hindringer og omveier.

Noen miljøer ved **Det humanistiske fakultet** driver med forskning på innsamlet spontan tale og tekst, med mål om å karakterisere språkbruk, syntaks, nøkkelord, osv. Et eksempel er ASK (Norsk Andrespråkskorpus) som inneholder tekster skrevet av studenter med norsk som andrespråk. Eksempler på talespråkskorpus er COLA og COLT som inneholder spontan tale fra ungdom på hhv. spansk og engelsk. Spontan tale og stiler inneholder ofte autobiografiske elementer og personrettede uttalelser som involverer andre personer, steder osv. Derfor blir slike materialer anonymisert på flere nivåer, bl.a. ved å fjerne eller maskere deler av de

opprinnelige opptakene eller tekstene. Et eksempel på sensitive taledata er det engelske ”Teenage health freak corpus”, som inneholder opptak fra samtaler mellom ungdom og helsepersonell. Selv om slike materialer ikke er tilgjengelige i sin opprinnelige form for de fleste forskerne, må materialene transkriberes og bearbeides av et team med forskere som har direkte tilgang. Under denne prosessen er det behov for strammere retningslinjer og sikker prosessering og lagring. Eksempelet illustrerer behovet for systemer for sikker behandling også utenfor de miljøene som hovedsakelig forvalter data om helseforhold.

Ved **Det juridiske fakultet** benyttes tradisjonelt ikke dokumenter som inneholder sensitive personopplysninger. I dommer og annen praksis der problemstillingen kunne tenkes å reise seg, er slik informasjon normalt luket ut før dokumentet kommer forskeren i hende. Det kan likevel ikke utelukkes at det også ved Det juridiske fakultet i enkelte tilfeller kan være behov for systemer som ivaretar hensyn til sikker databehandling som ledd i forskning.

4. Prosesser og løsninger ved andre universiteter, helseforetak og FHI

Gruppen har skaffet seg informasjon om tilsvarende løsninger ved noen av våre samarbeidsinstitusjoner og institusjoner vi kan sammenlignes med. Oversikten er ikke utfyllende. Det er vårt inntrykk at de fleste samarbeidende forskningsinstitusjoner har, eller er i ferd med å utvikle systemer for sikker behandling av sensitive data. Arbeidsgruppen antar at disse systemene om kort tid vil bli en del av institusjonenes vanlige IT-infrastruktur. Den samlede erfaringen med utvikling av slike systemer har allerede bidratt til å redusere utviklingskostnadene. Samtidig vil utviklingen ved andre institusjoner påvirke forskeres og tilsynsmyndighetenes forventninger til dataplattformene UiB kan tilby sine forskere.

Helse Vest har en løsning som ligner på den lagringsløsningen for UiB som ble beskrevet i Roknerapporten (se under). Helse Vest sin løsning driftes imidlertid i en sikker sone og er bare åpent for egne klientdriftede maskiner via helsenettet og gir dermed et høyt sikkerhetsnivå. UiB-ansatte som også er sykehusansatte benytter seg i stor grad av dette systemet ved at de behandler sensitive pasientdata på denne serverløsningen. For disse forskerne er dette en innarbeidet, sikker og god løsning.

Universitetet i Oslo utviklet først en løsning for et sikkert system (TSD 1.0) som ikke brukervennlig nok. De har nå videreutviklet denne til en ny løsning (TSD 2.0) som er beskrevet senere i denne rapporten. Systemet er ennå ikke kommet i ordinær drift (desember 2013). ELIXIR-miljøet på Institutt for informatikk ved UiB har knyttet seg opp mot TSD. TSD fremstår på mange måter som en nasjonal infrastruktur for sikker databehandling ved at den i stor grad er åpen for eksterne brukere, men det gjenstår å se hvor vellykket prosjektet blir. Systemet har på mange måter satt standard for utforming av systemer for sikker databehandling.

NTNU har utviklet et eget sikkert system for sikker behandling av genetiske data knyttet til HUNT-studien som kalles eGenVar. Systemet skal kunne tilby sikker databehandling til eksterne brukere. Systemet har likhetstrekk med TSD og LSP. Høyskolen i Bergen har også utviklet et lignede system.

Universitetet i Bergen har i dag forskjellige løsninger. Psykologisk fakultet har en løsning med et lukket nett helt adskilt fra internett. Ved IT-avdelingen har det vært tilbudt en løsning som

er beskrevet i Roknerapporten, men gruppen har vurdert at det er mulig å øke sikkerheten på enkelte punkt. Det er derfor utviklet en ny løsning (LSP) som er beskrevet senere i dokumentet. Dette systemet er blitt evaluert i en egen ROS-analyse og danner utgangspunkt for forslaget om et sikkert IT-system fra arbeidsgruppen.

Folkehelseinstituttet har et IT-system for sikker databehandling som er lukket og i praksis forutsetter at brukeren sitter innenfor et område som er fysisk sikret med adgangskort. Systemet har høyt sikkerhetsnivå og kan ikke nåes av brukere via internett.

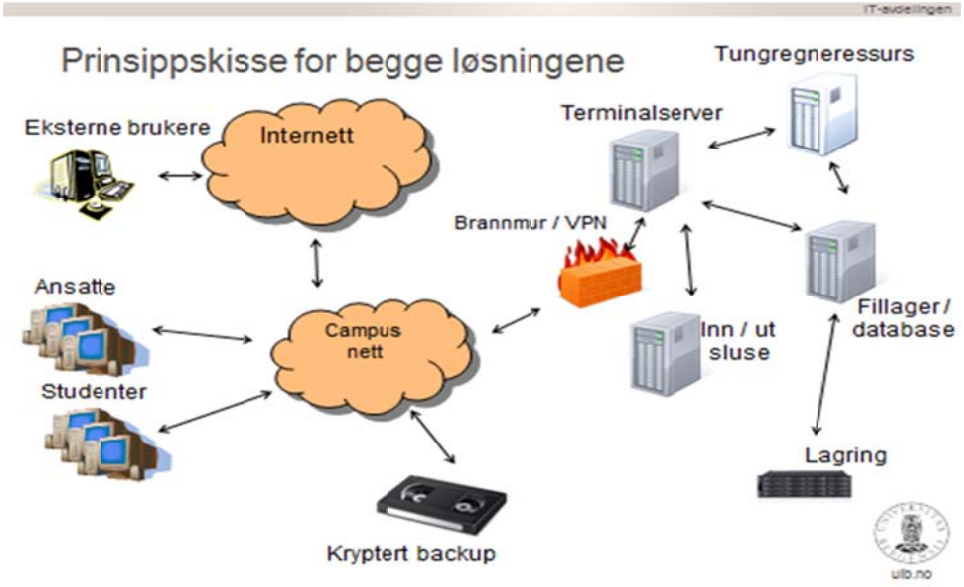
5. Vurdering av alternative tekniske løsninger for et sikkert IT-system

Rokne-gruppen skisserte en løsning som hadde sitt utspring fra den løsningen Helse Vest hadde på den tiden da rapporten ble skrevet. Denne løsningen bestod i to forskjellige katalogstrukturer der den ene inneholdt forskningsdata, mens den andre inneholdt koblingen mellom data og personer. Det skulle begrenses og registreres hvem som fikk tilgang til data på serveren og bare et fåtall personer skulle ha tilgang til kobling mellom person og data. Denne løsningen ble implementert, men er nå forkastet da sikkerhetsnivået i den løsningen ikke er vurdert som god nok innenfor rammen av UiB sitt nettverk. Data som er lagret i denne løsningen vil måtte overføres til ny løsning når denne er implementert.

Arbeidsgruppen har tatt som utgangspunkt at «Normen» skal være oppfylt for et sikkert IT-system. Det har i tillegg vært en forutsetning at systemet blir brukervennlig og oppleves som en forbedring av det datatekniske arbeidsmiljøet for forskeren. Forskere vil sette pris på enkel tilgang via internett, regnekraft, muligheten til å ha data på et sted og tilgang til god og oppdatert programvare.

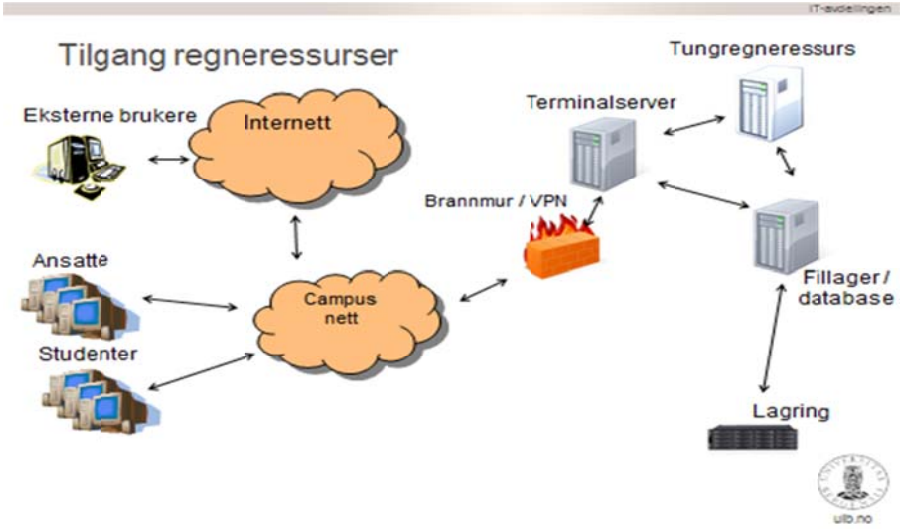
Prinsippskisse for TSD 2.0 (UiO: Tjenester for sensitive data) og LSP (UiB: Løsning for sensitive persondata)

Vi har valgt å betegne det nye systemet som gruppen foreslår med LSP (Løsning for sensitive persondata). UiO-systemet TSD 2.0 og LSP har mange likheter og kan i prinsippet beskrives likt. Skissene nedenfor gjelder for begge løsningene. Forskjeller i løsningene er beskrevet etterpå.



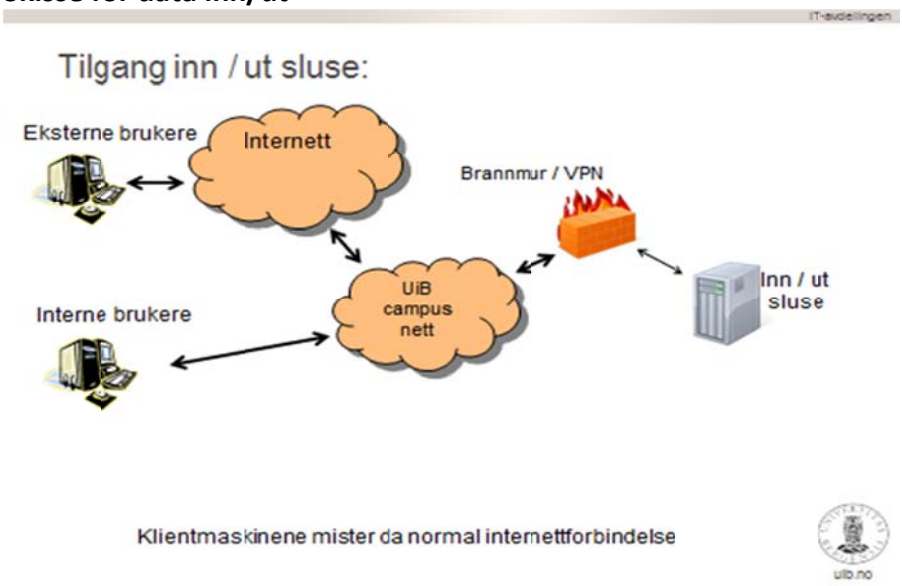
Funksjonalitet i begge systemene er i stor grad lik. Brukere får tilgang til ressurser gjennom en 2-faktor VPN-pålogging, og deretter gjennom et Windows terminalservervindu eller et SSH vindu til en Linux terminalserver. TSD baserer seg på kodekalkulatorer, mens LSP baserer seg på engangspassord pr SMS eller kodekalkulator for 2-faktorløsning. TSD har duplisert mange av infrastrukturkomponentene som trengs for å kjøre tjenesten innenfor brannmuren, mens LSP gjenbruker disse komponentene fra UiB's ordinære infrastruktur. TSD deler lagringsressursene med resten av UiO's lagringsbehov og er også koblet opp mot den nasjonale lagringsressursen Norstore. LSP har dedikert lagring på innsiden av brannmuren. TSD kjører virtualisering av servere og nettverk for å skille mellom prosjektene, mens LSP i dag kjører på en flat struktur.

Skisse for tilgang til regneressurser



Tilgang til regneressursene fungerer i prinsippet likt i begge løsningene. Man må først koble seg opp med 2-faktor VPN og deretter med SSH eller terminalserver. Regneressursene i begge løsningene kan i stor grad tilpasses brukernes behov. TSD tilbyr tungregnekapasitet, noe LSP så langt ikke har.

Skisse for data inn/ut



Det er bare definerte brukere som kan flytte data inn og ut av systemene i LSP og TSD 2.0. Dette gjøres gjennom et slusesystem der systemet logger navn på filer, innhold og hvilken bruker som har flyttet dataene. All trafikk her er kryptert. Prosjektledere gis tilgang til logger for flytting av data. Sensitive persondata som flyttes inn eller ut av systemet må være kryptert med en for tiden sterk nok krypteringsalgoritme. Forskerne vil ha behov for å få resultatfiler, for eksempel grafikk, ut av systemet. Disse filene vil også måtte hentes ut via filslusen. Dette vil trolig oppleves som mer tungvint enn dagens situasjon.

Utfyllende detaljer om TSD 2.0 (UiO)
TSD 2.0 er UiO sin løsning for lagring og behandling av sensitive personopplysninger. Denne er bygget for å kunne tilby tjenester på et nasjonalt nivå. Det er brukt 4 årsverk i 2 år for å utvikle løsningen. Dette er en full nyimplementasjon basert på TSD 1.0, som tidligere har vært tilbudt ved UiO. Løsningen tilbyr lagring av data, og ressurser til å behandle disse. Brukere får tilgang til dataene gjennom en Linux eller Windows maskin. For tyngre regneoppgaver tilbys det tilgang til et regnecluster dedikert til TSD 2.0. I tillegg til dette tilbys det muligheter for å lage spørreskjema, koblet mot Min ID, som leverer data inn i systemet på en sikker måte. TSD 2.0 er bygget opp mest mulig som en enkeltstående tjeneste som i liten grad benytter seg til andre tjenester ved UiO. Infrastruktur som er nødvendig for at tjenesten skal virke er i stor grad duplisert (Cerebrum, AD, DNS, DHCP, mm). Det er noen infrastruktur-komponenter som deles med resten av UiO sine IT-tjenester. Disse er lisensserver, OS oppdateringer, backup, CF-engine, og SAN. Sikkerhet i disse komponentene er løst med «pull»-funksjonalitet, kryptering og virtualisering for å hindre lekkasje mellom systemene. De forskjellige prosjektene skilles med egne virtuelle servere, og virtuelle nettverkssegmenter. Det er en begrensing på 200 vlan (hovedprosjekt) , men TSD har også muligheten på noe mer sikt å ”poole” prosjekter under ett VLAN, da med separasjon ivaretatt av IP-tables, nettgrupper, filgrupper og ACL´er. I skrivende stund er Windows beregningsressurser basert på en Windows 2012 server. Når man tilbyr tjenester til kunder ut over UiO utløser det en del lisensproblematikk og økte kostnader. F.eks SPSS krever concurrent-lisenser ved UiO for dette formålet.

Utfyllende detaljer om LSP (UiB)
LSP er UiB sin løsning for lagring og behandling av sensitive personopplysninger og ble i utgangspunktet designet for et prosjekt ved Institutt for global helse og samfunnsmedisin (IGS). Tidligere hadde UiB en enkel løsning som kun bestod i lagring av data med skille mellom identifiserende nøkkel og dataene som beskrevet i Roknerapporten. Data ble i denne løsningen lagret bak en brannvegg, men behandlet på vanlige klient-pcer. LSP-løsningen ligner mye på UiO sin løsning, men med mer bruk av infrastruktur-komponenter som er felles med resten av UiB sine IT-løsninger (Sebra, AD, DHCP, mm). Det er heller ikke virtuelle nettverkssegmenter som skiller prosjektene. Det er per dags dato ikke tungregneressurser i denne løsningen, men prosjektene har egne fysiske servere. I motsetning til UiO har UiB dedikert SAN-løsning som ikke er koblet opp til andre tjenester. Det er blitt foretatt en ROS analyse av IGS-løsningen.

6. Innfasing av et sikkert IT-system
LSP er i en fase hvor systemet blir utviklet mens det er et begrenset antall brukere inne i systemet fra Institutt for global helse og samfunnsmedisin og fra Institutt for økonomi. Det vil ikke bli gitt tilgang til nye brukere før designet av løsningen er endelig valgt. Det bør

kjøres en periode med eksisterende brukere for å få erfaring med bruken av systemet. Deretter kan dataene fases inn i systemet prosjekt for prosjekt. Dette bør skje institutt- eller fakultetsvis samtidig som det gjennomføres opplæringstiltak.

Brukere som ikke er ansatt ved UiB vil trenge en UiB-konto for å få tilgang («andre»-konto). Dersom de har ansettelsesforhold og klientmaskin hos en samarbeidende institusjon som et norsk universitet eller tilsvarende forskningsinstitusjon skal de kunne bruke sin egen klientmaskin til oppkobling mot systemet, gitt betingelser rundt beskyttelse mot virus etc. Aktuelle brukere som ikke har et slikt arbeidstakerforhold vil kunne utstyres med en UiB-klientmaskin for å kunne arbeide med LSP. For alle eksterne brukere må det utarbeides et avtaleverk om bruken av systemet. Dette vil innebære praktiske utfordringer og mulige ekstrakostnader men kan samtidig bidra til at kravene i Normen (www.normen.no) til såkalt hjemmekontor hvor bruker ikke sitter i det interne nettverket blir oppfylt for systemet. Studenter kan ikke få tilgang til systemet slik det nå er planlagt uten at de får en egen konto (”andre”-konto) ved et UiB-institutt og arbeider via en UiB-driftet maskin.

Rokne-rapporten inneholdt gode forslag til hvordan man kan administrere tilgang til data i den sikre løsningen. Rapporten foreslo at én person på institutt- eller fakultetsnivå ble oppnevnt som rekvirent for tilgang til løsningen, og tilsvarende at én person kan gi tilgang til data på prosjektnivå. Disse funksjonene kan godt fylles av en og samme person. Alle som skal ha tilgang til løsningen må ha en konto ved UiB som i dag opprettes av en «godkjenner» i Sebra. Slike autoriserte «godkjennere» finnes normalt ved hvert institutt, eller deles mellom institutter. Når en ny bruker skal ha tilgang til data i LSP, må prosjektleder ta kontakt med «godkjenneren» for å få be om slik tilgang. «Godkjenner» sender så forespørsel videre til IT-avdelingen. Denne modellen ble valgt ettersom IT-avdelingen ikke vil kunne forholde seg til alle prosjektledere. I første omgang må godkjenningen gjøres via et papirskjema. Det er ønskelig at dette i fremtiden håndteres gjennom elektronisk løsning.

Oppsummert vil en slik løsning gi mulighet for lagring og bruk av forskningsdata som tilfredsstiller norm for datasikkerhet. Den enkelte forsker vil også kunne jobbe på eksakt samme måte på sitt eget kontor ved UiB og utenfor UiB sitt nettverk via internett. Siden regneressursene vil finnes internt i UiB systemet, vil det i mange tilfeller kun være mindre tekstbasert (syntax) datastrøm som kreves for å kjøre analysene på server og få resultatene tilbake til bruker over internett. Systemet vil dermed stille lave krav til internetthastighet for den enkelte bruker (Edge-oppkobling vil gjøre nytten for de fleste behov). En felles løsning vil også gjøre at forskningsmiljø med letthet kan dele dataressurser som syntax, resultatfiler og bearbeidede datasett mellom forskerne. Det er enkelte sider ved systemet som nok vil kunne oppleves mer tungvint enn dagens praksis, slik som prosedyrene for å hente ut resultat og tekstfiler basert på utregninger. Videre krever systemet at alle brukere må være utstyrt med en UiB-brukerkonto og en UiB-klientmaskin eller tilsvarende. Vi er imidlertid av den oppfatning at fordelene med et slikt system etter en innkjøringsfase langt vil overgå ulempene med systemet.

7. Krav til oppbevaring av data ved UiB utenfor sikkert IT-system

Ved bruk av egne maskiner til behandling av sensitive persondata må disse sikres fysisk mot tilgang fra uautoriserte personer, og holdes frakoblet fra internett. Sikker databehandling oppnås i dag for mange prosjekter ved at det benyttes egne maskiner til behandling av

sensitive persondata og ved at disse sikres fysisk mot tilgang fra uautoriserte personer og holdes frakoblet fra internett. I tillegg benyttes forskjellige krypteringsrutiner. Slike rutiner er vanligvis avklart i forhold til REK eller Datatilsynet. Ansvaret for en daglige databehandlingen ligger dermed ofte i praksis hos prosjektleder. Mange prosjektledere vil derfor ønske seg et felles sikkert system, slik at prosjektleder kan være trygg på at datasikkerhet er håndtert på tilstrekkelig måte innen institusjonen sin ramme. En viktig utfordring for et felles system er å kunne oppnå samme fleksibilitet og brukervennlighet som forskere med egne systemer opplever å ha. Et felles sikkert IT-system må ha som ambisjon å erstatte alternative løsninger. Etter en innkjøringsfase for et felles sikkert system bør det vurderes om slike alternativer skal fases helt ut. Et alternativ er å utvikle klarere krav til slike løsninger.

Alle som benytter IT-tjenester hos andre leverandører, for eksempel TSD, skal påse at det foreligger en databehandleravtale som regulerer ansvar og rettigheter mellom driftsoperatør og Kunde/bruker. Mal og veileder for avtaler kan lastes ned fra Datatilsynet. https://www.datatilsynet.no/sikkerhet-internkontroll/databehandleravtale/

Direkte innlasting fra dataleverandør har ikke vært aktuelt til nå, men kan bli aktuelt i fremtiden dersom det skal kunne dokumenteres at data ikke blir oppbevart utenfor det sikre systemet. Data blir i dag i stor grad levert på kryptert CD-rom. Kryptering skal være gjennomført med godkjent programvare. IT-avdelingen gir råd om anbefalt og godkjent programvare.

8. Implikasjoner for internkontrollrutiner

Prosjektdatabase

Forskningssystemet legger stort ansvar for den daglige behandlingen av forskningsdata på prosjektleder. Den enkelte forskers ansvar er imidlertid knyttet til de rammebetingelsene forskningsansvarlig institusjon gir for sikker behandling både gjennom IT-systemene og internkontrollsystemet. UiB´s prosjektadministrative systemer bør suppleres med et system som gir oversikt over hvilke datafiler som behandles i hvert prosjekt og hvordan disse behandles. Et slikt system vil kunne dokumentere i hvilken grad UiB sine systemer for databehandling benyttes og eventuelt hvilke alternativer som er i bruk. Administrasjonen av et slikt system må koordineres mellom institutt, fakultet, forskningsavdeling og IT-avdeling.

Egenmelding

Gruppen foreslår at det innføres en ordning med egenmelding fra ansatte forskere kalt «Tilgang til forskningsfiler» hvor den enkelte melder til sitt institutt hvilke forskningsdata vedkommende har tilgang til. Formålet med egenmeldingen er å få bedre oversikt over hvilke dataressurser som finnes og brukes ved instituttene, bevisstgjøre den enkelte forsker på eget ansvar, sikre at de nye systemene tas i bruk, samt sikre at data fra forskningsprosjekter slettes når prosjektets avsluttes. Rutinen vil dokumentere hvordan data behandles ved institusjonen og dermed gi oversikt og muligheter for tiltak. Innmeldingen er tenkt å omfatte alle datafiler knyttet til prosjekter som har konsesjon fra Datatilsynet, godkjenning fra REK (eller tilsvarende) eller som i dag ville kreve REK-godkjenning. Det bør gjøres tydelig at ved tvil skal datatilgangen meldes. Et forslag til format på slik egenmelding følger nedenfor. Første runde av egenmelding kan godt gjøres på papir og lagres ved instituttet. Denne informasjonen må i seg selv behandles som sensitiv da den vil gi

informasjon om hvor data lagres. Vi foreslår at første runde gjennomfører ved et institutt i etterkant av at instituttets forskningsprosjekter er blitt faset inn i LSP-løsningen. Egenmeldingsrutinen skal gi et øyeblikksbilde og bør gjentas ved jevne mellomrom, for eksempel årlig. Ordningen kan innføres uavhengig av innfasingen av LSP. Informasjonen kan danne utgangspunkt for en projektdatabase ved instituttene eller fakultetene og vil kunne benyttes i fremtiden til å styrke internkontrollarbeidet. Dette tiltaket krever administrative ressurser.

Utkast til mal for egenmelding «Tilgang til forskningsfiler»
Egenmelding fylles ut av vitenskapelig ansatte eller teknisk-administrative med datatilgang og arkiveres ved instituttene. Meldingene kan danne grunnlag for, eller samordnes med en prosjektdatabase. Informasjonen om filer og lagring skal behandles som sensitiv. Forskningsgrupper bør samordne innmelding. Dersom samme fil er lagret flere steder, så skal hver fil meldes separat.

Datafil/plassering	Prosjekttittel	Prosjektleder	Godkjenning	Periode	Medarbeidere	Kommentarer

Egenmeldingen bør også registrere om forskeren har gjennomført kurs i, eller har fått informasjon om bruk av LSP-systemet ved UiB eller tilsvarende systemer.

9. Økonomi

Rokne-gruppen foreslo i sin rapport at en startet arbeidet med å lage et system for lagring og oppbevaring av forskningsdata slik IT-avdelingen skisserte i mai 2010. Det skisserte forslaget var basert på en løsning som Helse Vest hadde implementert. I ettertid ser en at denne løsningen ikke tilfredsstiller krav til sikkerhet og IT-avdelingen har derfor omarbeidet denne løsningen til det som nå kalles LSP. Dette har så langt ikke krevd tilleggsressurser for IT-avdelingen.

For å kartlegge sikkerheten i den nye LSP-løsningen, blir det med oppstart medio november 2013 foretatt en ROS-analyse av et eksternt firma som er ekspert på slike løsninger. Rapporten fra denne analysen vil fortelle om mangler i forhold til eksisterende oppsett og si noe om både hardware og timeressurser som må til for å tilfredsstille de krav vi setter til en sikker løsning for sensitive forskningsdata.

Til sammenligning har det tatt UiO 8 årsverk å bygge ut TSD så langt. I følge de ansvarlige hos UiO vil det kreve minst 4 årsverk for UiB å bygge opp en tilsvarende sikker løsning gitt at en kan arve og lære en del av det USIT allerede har tenkt og gjort.

Det er for tidlig å si eksakt hva oppbygging av en sikker løsning i full skala ved UiB vil koste, men et rimelig anslag vil følge av skissen under til bemannings- og utstyrsbehov:

1. Sikkerhetsansvarlig med ansvar for å gi råd, holde seg oppdatert på gjeldende trusselbilde, kjenne lovverk på området etc. IT-avdelingen har i budsjettforslag for 2014 bedt om å få omgjort hovedtyngden av de midler som i dag brukes på IT-sikkerhet til en slik stilling.
2. Overingeniør nettverk – oppbygging og vedlikehold av et sikkert nett krever både kompetanse og ressurser som ikke er tilgjengelig på i dag.
3. Overingeniør Windows – hovedsakelig økning av arbeidskapasitet.
4. Tentativt: dersom det kreves spesiell kompetanse på programvare for å tilfredsstille brukere av en sikker løsning, så kan det medføre et ytterlig bemanningsbehov.
5. Kapasitet på brukerstøtte og opplæring
6. Det vil også være behov for utstyr. Budsjett for dette vil bli utarbeidet etter at behovsomfanget er kartlagt.

Stillingene i punkt 2-4, vil alle være stillinger som er nøye knyttet til fagnær virksomhet og vil være nært knyttet til det ordinære tilbudet og driften fra IT-avdelingen.

Dersom studenter skal kunne benytte løsningen med sin studentkonto, må deler av løsningen få nytt design og bygges om. Dette vil utløse både maskinkostnader, men først og fremst innsats av arbeidskraft.

Drift av systemet vil også kreve øket administrativ innsats ved institutter, fakulteter, FA og IT-avdelingen. Dette kan godt sees i sammenheng med internkontrollsystemet ved UiB. Informasjons- og opplæringsbehovet vil også kreve noen ekstra ressurser i en oppstartfase.

10. Informasjonsbehov internt og eksternt

Det vil oppstå et sterkt informasjonsbehov hos forskningsmiljøene når dette systemet innføres. Informasjon om systemet og om tilgangen til systemet må gjøres lett tilgjengelig på it.uib.no. I forbindelse med innfasing av systemet bør det satses på informasjon og opplæring ved hvert enkelt institutt. Det bør utarbeides et kursopplegg for dette formålet. Uavhengig av opplæring, må det forventes at det oppstår frustrasjoner og behov for ekstra brukerstøtte. Det bør settes tidsfrister for innfasing og evaluering av systemet. Det bør også planlegges en markering av at systemet er etablert når det er kommet ordentlig på plass.