KONTROLL AV LOGGER FRA BEHANDLINGSRETTEDE HELSEREGISTRE

Universitetet i Oslo
Det juridiske fakultet

Kandidatnummer: 694
Leveringsfrist: 26.04.2011

Til sammen 17232 ord

26.04.2011

Innholdsfortegnelse

1 Problemstilling

Norske sykehus behandler personopplysninger om alle pasienter de har behandlet. Mye av denne informasjonen finnes i det elektroniske journalsystemet. Informasjon om personers helseforhold er definert som sensitive opplysninger i personopplysningsloven § 2 nr. 8 bokstav c, og behandling av helseopplysninger i elektroniske journalsystemer er underlagt reglene i helseregisterloven og personopplysningsloven med forskrift. [1]
For blant annet å sikre pasientenes personvern[2], er sykehusene pålagt å sørge for tilfredsstillende [3] informasjonssikkerhet ved behandling av opplysningene. Hva som er tilfredsstillende informasjonssikkerhet når sykehusene behandler helseopplysninger, må vurderes med utgangspunkt i reglene i helseregisterloven og personopplysningsforskriften.
I tillegg finnes det andre regler i helseregisterloven og helsepersonelloven som har som formål å beskytte de registrertes personvern. Dette er reglene om taushetsplikt og tilgang til opplysninger i helseregistre i helseregisterloven, og reglene om profesjonsbestemt taushetsplikt i helsepersonelloven. Til sammen inneholder disse tre lovene et sett grunnkrav som må oppfylles før sikkerhetstiltakene kan anses å være tilfredsstillende, men det er i stor grad sykehusene som avgjør hvilke sikkerhetstiltak som skal implementeres, og i hvilken grad.
Personopplysningsforskriftens kapittel 2 inneholder utfyllende bestemmelser til helseregisterloven § 16 om informasjonssikkerhet. Forskriftens §§ 2-8 og 2-14 stiller krav om logging av henholdsvis autorisert tilgang og forsøk på uautorisert tilgang. Formålet med reglene er å beskytte de registrertes personvern ved å forhindre hendelser som har konsekvenser for helseopplysningenes konfidensialitet, integritet og tilgjengelighet.
Når man ser disse reglene i sammenheng med reglene om tilgang til helseopplysninger i helseregisterloven, dukker det opp noen interessante problemstillinger:

---

[1] Helseregisterloven § 36 slår fast at personopplysningsloven med forskrift gjelder som utfyllende bestemmelser til reglene i helseregisterloven.
[2] Helseregisterloven § 1, jf. personopplysningsloven § 1
[3] Helseregisterloven § 16

- Hvor aktive er sykehusene forpliktet til å være når det gjelder bruk av logger til å avdekke brudd på tilgangsbestemmelsene i helseregisterloven §§ 13 og 13a?
- Hva må logges for å oppfylle kravene til logging i personopplysningsforskriften?
- Hvilke metoder for logganalyse egner seg?

Jeg vil i denne oppgaven beskrive tre strategier som har vært brukt eller forsøkt brukt i logganalysesammenheng, og vurdere hvordan de er egnet til å oppfylle kravene i loven.

2 Avgrensning

2.1 Forholdet til ansattes personvern

Oppfølging av logger kan innebære et kontrolltiltak overfor de ansatte. Arbeidsmiljøloven kapittel 9 inneholder regler om kontrolltiltak i virksomheten. Utgangspunktet er at en virksomhet bare kan iverksette kontrolltiltak når kontrolltiltaket er saklig begrunnet i virksomhetens forhold, og tiltaket ikke innebærer en uforholdsmessige belastning for de ansatte.[4] Hvilke krav som må stilles for at kontrolltiltaket skal være rettmessig, vil avhenge av behovet for kontrollen, kontrolltiltakets art, samt hvor inngripende det vil virke i forhold til den enkelte.[5] Saklighetskravet innebærer at kontrolltiltaket må være saklig i seg selv, og saklig overfor den ansatte som blir utsatt for kontrolltiltaket. Forholdsmessighetskravet innebærer at man ikke bare skal vurdere om det enkelte tiltak er uforholdsmessig, men også se på summen av kontrolltiltak i virksomheten.[6]
Hvis kontrolltiltaket innebærer behandling av personopplysninger om de ansatte, må behandlingen ha hjemmel i personopplysningsloven, og følge denne lovens regler for behandling av personopplysninger.[7] Kontrolltiltaket skal drøftes med arbeidstakernes tillitsvalgte.[8]

[4] Arbeidsmiljøloven § 9-1 første punkt
[5] Ot.prp. nr. 49 (2004-2005) s. 144
[6] Ot.prp. nr. 49 (2004-2005) s. 314
[7] Arbeidsmiljøloven § 9-1 andre punkt
[8] Arbeidsmiljøloven § 9-2 første punkt

Jeg kommer ikke nærmere inn på forhold rundt de ansates rettigheter i denne oppgaven, men reglene om kontrolltiltak og ansattes personvern vil være viktige når et sykehus skal innføre logganalyse.

2.2 Andre helseregistre

Temaet i denne oppgaven er analyse av logger fra det elektroniske journalsystemet. Det finnes andre behandlingsrettede helseregistre hvor det også kan være nyttig å benytte logganalyse, men disse systemene vil ikke bli diskutert i denne oppgaven. Oppgaven tar heller ikke for seg analyse av logger fra helseregistre som ikke er behandlingsrettede.

3 Definisjoner

3.1 Elektronisk pasientjournal

En elektronisk pasientjournal blir ført elektronisk i stedet for på papir. Dette skjer i et datasystem som er spesiallaget for å oppbevare og organisere elektroniske pasientjournaler, for eksempel DocuLive EPJ som er i bruk ved store deler av Oslo universitetssykehus (Rikshospitalet, Radiumhospitalet, Ullevål sykehus).

I forskrift om pasientjournal er en journal definert som ”en samling eller sammenstilling av nedtegnede/registrerte opplysninger om en pasient i forbindelse med helsehjelp, jf. helsepersonelloven § 40 første ledd”. Helsepersonell er pålagt dokumentasjonsplikt i helsepersonelloven § 39. Journalen skal inneholde nødvendige og relevante opplysninger om pasienten, jf. helsepersonelloven § 40. Det skal som hovedregel opprettes én journal per pasient, jf. pasientjournalforskriften § 5.
Det elektroniske pasientjournalsystemet er ett eksempel et behandlingsrettet helseregister, jf. helseregisterloven § 2 nr. 7.

3.2 Logg

En logg (eller et hendelsesregister) er en oversikt over aktivitet i et datasystem eller dataprogram. I en elektronisk pasientjournal vil en logg inneholde informasjon om

oppslagene brukerne av journalsystemet har gjort. Et oppslag kan for eksempel se slik ut (her fordelt på to linjer på grunn av plassmangel):

ID	Nr	LoginID	RecordID	UserName	Fornavn	Mellom-navn	Etternavn	Tittel	Avdeling	Yrkes-gruppe	Funksjon
01	0001	kndorm	NULL	Nordmann, Kari	Kari	NULL	Nordmann	Sekretær	Kreftklinikken	Helse-sekretær	Tilgang Scanning

PatientName	BirthNo	DocumentName	BeginTime	EndTime	AccessType	Årsak	Logtime
NORDMANN, OLA	01011111111	NORDMANN, OLA	2011-02-19 12:45:00.000	2011-02-21 12:45:00.000	Read	Behandle henvisning/søknad	2011-02-19 12:45:00.000

Tabell 1. Eksempel på loggoppføring

Dette eksempelet på en loggoppføring er hentet fra DocuLive EPJ som brukes ved Oslo universitetssykehus. Logger hentet ut fra andre journalsystemer kan se anderledes ut.

4 Logging

4.1 Informasjonssikkerhet

Behandling av helseopplysninger stiller særlige krav til sikring av konfidensialitet, tilgjengelighet og integritet. Sykehuset er forpliktet etter helseregisterloven og personopplysingsforskriften[9] til å implementere nødvendige sikkerhetstiltak og sørge for at tiltakene gir tilfredsstillende informasjonssikkerhet.

De overordnede kravene til informasjonssikkerhet i helseregistre finnes i helseregisterloven § 16. Den sier at databehandlingsansvarlig ”gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet”, og at tiltakene skal dokumenteres. Tilfredsstillende er i denne sammenheng en rettslig standard, og hva som ligger i uttrykket varierer fra tilfelle til tilfelle, og kan også forandre seg over tid. Hva som anses som tilfredsstillende informasjonssikkerhet på et sykehus må sees i lys av formålsbestemmelsen i helseregisterloven, som sier at ”loven skal sikre at helseopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på

[9] Helseregisterloven § 36 slår fast at personopplysningsloven med forskrift gjelder som utfyllende lovgivning til helseregisterloven.

helseopplysninger"[10] og bestemmelsen i helseregisterloven § 13 som sier at tilgang til helseopplysninger bare kan gis "i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt". Etter at helseregisterloven ble vedtatt fikk den en ny bestemmelse i § 13a. Bestemmelsen gjør det forbudt å "lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter denne loven uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift". Forbudet har samme formål som taushetsplikten[11], og Helse- og omsorgsdepartementet uttalte at bestemmelsen måtte "ses i sammenheng med de øvrige personvernbestemmelsene i helselovgivningen, og særlig helseregisterloven § 13".[12] Dette innebærer at sikkerhetsmekanismene ikke bare må bidra til å oppfylle kravene i § 13, men også i § 13a.

Loven sier ikke i detalj hvilke mekanismer som er aktuelle, men for å avgjøre hvilke tiltak som vil gi tilfredsstillende informasjonssikkerhet, må det gjøres en konkret vurdering både for hvert enkelt system, og for informasjonssystemet som helhet. [13] I tillegg må tiltak som er gitt i medhold av loven, for eksempel i personopplysningsforskriften, vedtak fra Datatilsynet eller i konsesjoner, inkluderes. Tiltakene kan være av organisatorisk, systematisk, teknologisk, teknisk og annen art. [14] At tiltakene skal være planlagte og systematiske innebærer at implementeringen av tiltakene må komme som et resultat av en helhetlig vurdering av hvilke trusler som kan sette pasientenes personvern i fare. Det betyr sykehuset må ha en formening om hva som kan representere en fare for informasjonssikkerheten før behandlingen av helseopplysninger starter. Kravet til systematikk innebærer at arbeidet med informasjonssikkerhet må ikke være preget av tilfeldigheter, men følge på forhånd definerte prosedyrer. [15]

De overordnede kravene i helseregisterloven § 16 danner rammeverket for reglene om informasjonssikkerhet i personopplysningsforskriften. Forskriftens § 2-1 annet ledd sier at de planlagte og systematiske tiltakene skal "stå i forhold til sannsynligheten for og

[10] Helseregisterloven § 1 siste punktum
[11] Ot.prp. nr. 25 (2007-2008) s. 64
[12] Ot.prp. nr 25 (2007-2008) s. 65.
[13] Personopplysningsforskriften § 2-7
[14] Schartum, Bygrave (2004) s. 141
[15] Schartum (2005) s. 120

konsekvens av sikkerhetsbrudd". Sykehuset må således vurdere sannsynligheten for, og konsekvensene av, forskjellige sikkerhetsbrudd før de bestemmer seg for hvilke tiltak de vil innføre. I tillegg må de vurdere med hvilket omfang og hvilken intensitet tiltakene skal innføres.

§ 2-3 pålegger den databehandlingsansvarlige å utarbeide sikkerhetsmål og en sikkerhetsstrategi. Sikkerhetsmålene skal inneholde formålet med behandlingen av personopplysninger og overordnede føringer for bruk av informasjonsteknologi.De kan for eksempel beskrive hvordan virksomheten forholder seg til opplysninger som må sikres med hensyn til konfidensialitet og tilgjengelighet.[16] De bør defineres presist, og være målbare.[17]
Sikkerhetstrategien skal inneholde en beskrivelse av valg og prioriteringer i sikkerhetsarbeidet. Den vil blant annet omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet.[18] Strategien skal beskrive hvordan virksomheten skal nå sikkerhetsmålene.

I § 2-4 blir virksomheten pålagt å gjennomføre risikovurderinger. Formålet med risikovurderingene er å kartlegge sannsynligheten for og konsekvensene av en hendelse som fører til brudd på konfidensialitet, tilgjengelighet og integritet. Slike hendelser kalles sikkerhetsbrudd. Virksomheten er pålagt å utarbeide en oversikt over hvilke personopplysinger som behandles, og bestemme hva som er akseptabel risiko for sikkerhetsbrudd.[19] Uttrykket "akseptabel risiko" er en rettslig standard, hvis innhold må fastsettes i hvert enkelt tilfelle. Hva som er akseptabel risiko vil avhenge av typen personopplysninger som blir behandlet, hva behandlingen består i og hva som er formålet med den. I tillegg vil spesiallovgivning om behandling av bestemte typer personopplysninger ha betydning. Den akseptable risikoen må defineres slik at den gir tilfredsstillende informasjonssikkerhet, jf. hovedregelen i helseregisterloven § 16. Etter at virksomheten har bestemt hva som er akseptabel risiko for sikkerhetsbrudd, må den reelle risikoen for at sikkerhetsbrudd oppstår analyseres. Da må virksomheten ha

[16] Datatilsynets kommentarer til sikkerhetsbestemmelsene i personopplysningsforskriften s. 7
[17] Schartum (2005) s. 121
[18] Datatilsynets kommentarer til sikkerhetsbestemmelsene i personopplysningsforskriften s. 7
[19] Personopplysningsforskriften § 2-4 første ledd

oversikt over trusselbildet, og vurdere for hver behandling av personopplysninger hvor stor risiko det er for at de forskjellige truslene slår til og hvilke konsekvenser det kan få. Ved vurderingen av konsekvensene må man se hen til formålet med lovgivningen, som er å beskytte personlig integritet, privatlivets fred og kvaliteten på dataene.[20] Det er altså den poteniselle konsekvensen for disse tre momentene som skal analyseres. Den reelle risikoen må sammenlignes med den akseptable risikoen, og der hvor den reelle risikoen er høyere enn den akseptable, må virksomheten implementere sikkerhetstiltak som får risikoen ned på akseptabelt nivå, og dermed bidrar til tilfredsstillende informasjonssikkerhet.

4.2 Krav om logging

Hovedreglene om logging finnes i personopplysningsforskriften §§ 2-8 og 2-14:

- § 2-8 sier at *autorisert bruk av informasjonssystemet skal registreres*
- § 2-14 sier at *sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet*, og gjøre det mulig å *oppdage forsøk på slik bruk*. I tillegg sier bestemmelsen at *forsøk på uautorisert bruk av informasjonssystemet skal registreres*.

I tillegg forutsettes eksistensen av en logg i helseregisterloven § 13 siste ledd, som gir en pasient rett til utskrift av tilgangsloggen fra sin journal. Denne bestemmelsen ble tatt inn i helseregisterloven i 2009 sammen med en endring som gjør at det ved forskrift kan åpnes for tilgang til behandlingsrettede helseregistre fra ansatte ved andre virksomheter.[21]

Selv om påleggene er absolutte, sier forskriften ingenting om hvordan loggene skal brukes, hva loggene skal inneholde eller hvordan de skal følges opp. Bestemmelsene må ses i sammenheng med § 2-11 som sier at det ”skal treffes tiltak mot uautorisert innsyn i opplysninger hvor konfidensialitet er nødvendig”.

For sykehusenes del vil dette si at de er forpliktet til å logge tilgang til journalsystemet, men hvordan loggene skal brukes, hva som skal logges og hvordan loggene skal følges opp vil avhenge av vurderingene som gjøres i sikkerhetsmålene, sikkerhetsstrategien og risikovurderingen. Disse vurderingene kan variere fra sykehus til sykehus avhengig av blant annet hvilke andre sikkerhetstiltak som er på plass og hvordan tilgangen til journalen er organisert. Men sykehusene kan ikke velge å ikke logge i det hele tatt.

[20] Helseregisterloven § 1 siste punktum
[21] Se helseregisterloven § 13 andre ledd og punkt 5.1

Begge de to største journalsystemene som er i bruk på norske sykehus i dag (DIPS og DocuLive) logger tilgang til elektroniske pasientjournaler. Vanligvis skjer registreringen både på det tidspunktet brukeren autentiserer seg, og for hvert oppslag brukeren gjør. Hvert oppslag blir liggende som én linje i loggen, og inneholder informasjon om hva som ble gjort, hvem som gjorde det og når vedkommende gjorde det. Loggen ligger i journalsystemets database, og man kan enten ta ut loggen for én bestemt pasient, eller hente ut logger over alle oppslag som er gjort, uavhengig av hvilken pasient det gjelder.

5 Kontroll av logger

5.1 Autorisasjon og autentisering

Sikkerhetsreglene i personopplysningsforskriften § 2 baserer seg på et prinsipp om at ingen skal ha tilgang til opplysninger de ikke er autorisert til å få tilgang til. Problemet er å finne gode tekniske tiltak for å sikre dataene mot innsyn og endring. I denne sammenhengen kan det være nyttig med noen definisjoner:

Autorisasjon: Begrepet autorisasjon knytter seg i denne sammenhengen til helseregisterloven og helsepersonellovens regler om lovlig tilgang til helseopplysninger. For at en person skal være autorisert for tilgang til journalsystemet, må kriteriene for tilgang til helseopplysninger i helseregisterloven § 13 være oppfylt. Det innebærer at man må være ansatt hos den databehandlingsansvarlige eller en databehandler, og ha behov for tilgang til journalsystemet i arbeidet sitt. I 2009 ble § 13 endret slik at det er mulig å få tilgang til behandlingsrettede helseregistre på tvers av virksomheter. Slik tilgang forutsetter at det blir gjort unntak i forskrift fra regelen om instruksjonsmyndighet i § 13 første ledd første punktum. I tillegg må pasienten ha gitt sitt uttrykkelige samtykke for at tilgang på tvers skal kunne gis.[22]

[22] Helseregisterloven § 13 andre og tredje ledd.

For at det enkelte oppslaget som gjøres i journalsystemet skal være lovlig, må oppslaget være begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp, eller ha særskilt hjemmel i lov eller forskrift.[23]

Autentisering: Dette er prosessen som identifiserer brukeren, og gjør at brukeren får tilgang til sykehusets journalsystem. I journalsystemet skjer dette ved at brukeren oppgir sitt personlige brukernavn og passord. Systemet sjekker brukernavn og passord opp mot en brukerkatalog, og hvis de er riktige, får brukeren tilgang til journalsystemet.

5.2 Forskjellige typer tilganger

Personell regnes som autorisert til å få tilgang til personopplysninger når de får tildelt brukernavn og passord i journalsystemet. De er da autorisert for tilgang i den utstrekning den rollen de har fått tildelt har tilgang. Alt helsepersonell ved et sykehus har i utgangspunktet tilgang til journalsystemet, og kan slå opp opplysninger om enkeltpasienter. Men det vil ikke si at hvert enkelt som gjøres, regnes som et lovlig oppslag. Per i dag finnes det ikke tekniske tiltak som sikrer at personellet bare får gjort lovlige oppslag. Den enkelte ansatte må selv avgjøre om han har hjemmel til å gjøre oppslag eller ei i hvert enkelt tilfelle. Dette innebærer at journalsystemets logg inneholder informasjon om hvem som har slått opp i en pasients journal, men ikke informasjon om oppslaget var lovlig.

Den grunnleggende autorisasjonen er styrt av sykehuset, og skjer ved at hver bruker som opprettes tilknyttes en rolle og en avdeling. Rollene tilsvarer helsepersonellets stilling, f.eks. lege, sykepleier eller helsesekretær. Rollen blir så knyttet til avdelingen helsepersonellet arbeider ved. Dermed får helsepersonellet mulighet til å slå opp alle pasienter som er innlagt ved den avdelingen han eller hun jobber på, eller annen tilgang i den utstrekning sykehuset mener det er nødvendig. Ved denne typen autorisasjon tar sykehuset en beslutning om hvor vid tilgang den ansatte trenger før den ansatte får tilgang til journalsystemet.

I mange tilfeller behandler helsepersonell pasienter som ikke er registrert som innlagt på deres avdeling. Dette kan være når flere avdelinger er involvert for å gi pasienten best mulig behandling, eller når avdelinger som ikke har egne sengeposter, som radiologi og anestesi, er involvert i behandlingen. Helsesekretærer som gjør

[23] Helseregisterloven § 13a og helsepersonelloven § 21a

administrativt arbeid på vegne av en klinikk eller avdeling har ofte behov for tilgang til journalene til pasienter som er skrevet ut, for eksempel for å skrive epikriser.
Man benytter da en tilgangsmekanisme som kalles "aktualisering". Den fungerer slik at helsepersonellet søker opp en pasient ved hjelp av fødselsnummer, og angir en grunn for hvorfor det er nødvendig å få tilgang til pasientjournalen. Brukere kan ha tillatelse til å bruke aktualisering i hele journalsystemet, bare i sin klinikk eller ikke i det hele tatt. Slik kan helsepersonell autorisere seg selv for å få tilgang til helseopplysninger.
Et problem med aktualisering er at helsepersonellet konsekvent får en mulighet til å gjøre oppslag det ikke har hjemmel for. Aktualisering var i utgangspunktet ment som en tilgangsmekanisme som skulle brukes i unntakstilfeller. I den sammenheng gjennomførte Rikshospitalet i 2007 et prosjekt sammen med Universitetet i Oslo for å undersøke bruken av aktualisering. Analyser av logger som ble gjort i prosjektet viste at aktualisering ble brukt som tilgangsmetode i 14% av oppslagene. Intervjuer med ansatte viste at det er mange årsaker til hvorfor ansatte bruker aktualisering som metode for å slå opp i journal, og at aktualisering brukes som et ledd i ordinær pasientbehandling, og ikke er unntakstilfeller. Noen av årsakene som ble nevnt er planlegging for pasienter som skal inn til operasjon, oppfølging før og etter operasjon, arbeide på poliklinikk, registrere søknader om innleggelse og kvalitetskontroll. Et tilsyn som Statens Helsetilsyn og Datatilsynet gjorde ved Haukeland universitetssykehus i 2006 viste at antallet aktualiseringer på enkelte pasienter var så høyt som 1/3 av de totale oppslagene.[24] Det kan diskuteres om en organisering av tilganger som medfører en så høy bruk av aktualisering som tilgangsmetode oppfyller tilgangsbestemmelsene i helseregisterloven §§ 13 og 13a og kravene til organisering av journalsystemet i pasientjournalforskriften § 4. Om helsepersonell skal ha anledning til å autorisere seg selv for tilgang til store mengder helseopplysninger uten at den databehandlingsansvarlige har tatt en avgjørelse om å tildele autorisasjonen er tvilsomt. På den andre siden kan en vid aktualiseringstilgang kombinert med opplæring og bevisstgjøring av brukerne være vel så bra som at man er autorisert for en veldig vid tilgang til å gjøre vanlige oppslag. Ved riktig bruk kan aktualiseringslogger være nyttige for å synliggjøre de tilfellene hvor helsepersonell har behov for tilganger utover de de er autorisert for.

[24] Rapport frå tilsyn med informasjonstryggleiken ved pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS ved Helse Bergen HF, Haukeland universitetssjukehus

Det synes å variere i hvilken grad sykehusene legger opp til at aktualisering skal brukes som en ordinær tilgangsmetode, og ikke bare i unntakstilfeller. Tilsynet ved Haukeland universitetssykehus og et tilsyn ved Akershus universitetssykehus i samme år avdekket sviktende tilgangsstyring ved begge sykehusene. På Haukeland i forbindelse med utstrakt rett for personalet til å bruke aktualisering, og på Ahus i forbindelse med for vide tilganger.[25] Ahus begrunnet de vide ordinære tilgangene med et ønske om å unngå "vesentlig behov for blålys". På Haukeland var tilgangene i journalsystemet organisert så selektivt som mulig, men det framgår ikke av tilsynet om den vide aktualiseringsretten har sammenheng med dette.
Uansett hvordan tilgangen til journalsystemet er organisert, er det et generelt problem at tilgangene er for vide. Datatilsynet skriver i en rapport fra 2009 at "Tilsynets kontroller har vist at både helsepersonell og andre ansatte i helsesektoren gjennomgående har alt for vid tilgang til å tilegne seg pasientopplysninger i den elektroniske journalen".[26]

Det er flere grunner til at tilgangene i journalsystemet er konfigurert slik de er. Viktigst er avveiningen mellom opplysningenes konfidensialitet og tilgjengelighet. Helseregisterloven, personopplysningsloven og personopplysningsforskriften stiller like strenge krav til sikring av konfidensialitet og tilgjengelighet. Hvilket hensyn som vektlegges må bero på en konkret vurdering i hvert enkelt tilfelle. På den ene siden er det viktig for tilliten til helsevesenet at sykehuset klarer å sørge for at tilgang til helseopplysninger skjer i overensstemmelse med gjeldende lover og regler. På den andre siden er det svært viktig for pasientbehandlingen at helsepersonellet har tilgang til de opplysningene de måtte trenge i en behandlingssituasjon.
Det er flere momenter som spiller inn når sykehuset gjør avveiningen mellom konfidensialitet og tilgjengelighet. Alle som har tilgang til journalsystemet er pålagt taushetsplikt.[27] Det vil si at selv om de skulle få tilgang til helseopplysninger de ikke har behov for, kan de ikke spre denne kunnskapen videre. Sykehuset driver også opplæring av ansatte, og har organisatoriske tiltak på plass som skal sørge for at ansatte

[25] Rapport frå tilsyn med informasjonstryggleiken ved pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS ved Helse Bergen HF, Haukeland universitetssjukehus og Rapport fra tilsyn med konfidensialiteten og tilgjengeligheten til elektronisk pasientjournal ved Akershus universitetssykehus HF.
[26] Sviktende tilgang i elektroniske pasientjournaler? Lovforslag om å tillate direkte tilgang til pasientjournaler på tvers av virksomhetsgrensene. Rapport fra Datatilsynet s. 4
[27] Helseregisterloven § 15 første og annet ledd

vet hvilke regler som gjelder for oppslag i journal.
Sykehuset må også vurdere konsekvensene for pasienten dersom opplysninger utleveres kontra konsekvensene hvis helsepersonell ikke får tilgang til nødvendige opplysninger. Konsekvensene av en utlevering er krenkelse av personvernet. I enkelte tilfeller kan det ha potensielt ødeleggende konsekvenser hvis helseopplysninger havner i feil hender. Konsekvensene av at helseopplysninger ikke er tilgjengelig for helsepersonell når de trenger det kan være feilbehandling eller ingen behandling. Dette kan føre til dårligere helse for pasienten, og i verste fall tap av liv.
Et annet hensyn som må ivaretas er effektivitetshensynet. Dersom sykehuset skal sørge for at alt helsepersonell kun har tilgang til helseopplysninger der hvor de er direkte involvert i behandlingen, må sykehuset til enhver tid ha oversikt over hvilket helsepersonell som er involvert i behandlingen av hvilke pasienter. Dette ville føre til store utfordringer for administrasjonen, ettersom de til enhver tid må kunne knytte riktig pasient til riktig helsepersonell på personnivå. Dette vil igjen kunne føre til at helsepersonell ikke har tilgang til opplysninger de har behov for.

5.3 Loggkontroll som sikkerhetstiltak

En konsekvens av at tilgangene i journalsystemet gjennomgående er for vide, er at sykehuset må ha organisatoriske og tekniske tiltak for å forhindre at helsepersonell tilegner seg informasjon de ikke har lovlig tilgang til. Organisatoriske tiltak finnes i form av interne rutiner og regelverk, og i form av opplæring og bevisstgjøring av brukere. Erfaringer viser at de fleste som er ansatt som helsepersonell har et bevisst forhold til taushetsplikten, og gjør sitt beste for å unngå å bryte den.[28] På den tekniske tiltaksfronten har det vært liten framgang. Sykehusene er pålagt å logge autorisert og forsøk på uautorisert bruk av journalsystemet, men loggene krever oppfølging for å være nyttige verktøy. Rutinene for loggjennomgang ved norske sykehus er varierende både med hensyn til hvem som foretar kontrollen og hvor hyppig kontrollen skjer.[29] Hovedregelen synes å være at aktualiseringslogger gjennomgås, mens det bare tas stikkprøver av loggene over vanlige oppslag. Rikshospitalet hadde for eksempel inntil

[28] Andresen, Aasland (2008)
[29] Rapport frå tilsyn med informasjonstryggleiken ved pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS ved Helse Bergen HF, Haukeland universitetssjukehus og Rapport fra tilsyn med konfidensialiteten og tilgjengeligheten til elektronisk pasientjournal ved Akershus universitetssykehus HF.

nylig rutiner som sa at aktualiseringslogger skal gjennomgås manuelt minimum hver tredje uke.[30] Hovedgrunnen til at aktualiseringsloggene velges ut, er fordi denne tilgangen i utgangspunktet har blitt ansett som en tilgangsmekanisme som skal brukes i unntakstilfeller. I tillegg er manuell loggoppfølging svært tidkrevende, og å gå igjennom alle oppslag lar seg ikke gjøre.

5.3.1 Målsetning

For å kunne etablere velfungerende metoder som skal brukes i loggkontroll, må sykehuset ha et klart målbilde. Hvilket fokus skal man ha når man gjennomfører kontrollen? Skal man satse på å ta de mest åpenbare taushetspliktbruddene, eller skal man ha som målsetning å avdekke alle oppslag som mangler hjemmel? Hvordan skal resultatene fra loggkontrollen brukes? Hvordan skal de følges opp? Hvor omfattende rapporter er det mulig å forholde seg til?
Svarene på disse spørsmålene vil ha mye å si for hvilke avgjørelser man tar i forbindelse med andre problemstillinger knyttet til loggkontroll og oppfølging av den, som for eksempel hvilke kildedata man skal ha med og hvor god datakvaliteten må være.

5.3.2 Utgangspunkt for kontrollen

Hovedproblemet forut for en loggkontroll er at når en bruker først har tilgang til journalsystemet, er det vanskelig å bruke loggene til å skille mellom berettigede og uberettigede oppslag. Ettersom autorisasjonen til å bruke journalsystemet blir gitt ved tildeling av brukernavn og passord, vil korrekt autentiserte oppslag ikke gi noe informasjon som kan fortelle om tilgangen er lovlig eller ikke lovlig.
For å kunne avsløre uberettigede oppslag, må man derfor ha en oppfatning av hva som kjennetegner dem. Ofte fattes det mistanke til oppslag som gjøres mellom avdelinger, oppslag som er gjort mens den ansatte ikke var på vakt eller oppslag som er gjort etter at pasienten er skrevet ut. Realiteten er at arbeidsforholdene på et sykehus kan være uforutsigbare. Mange som er ansatt ved sykehus opplever å ha forskjellig ansvar avhengig av hvilken vakt de går, eller de vikarierer på en annen avdeling enn sin egen hvis det er behov for det. I tillegg kan det oppstå uventede situasjoner hvor vanlige

[30] Intern rutine, Rikshospitalet

prosedyrer ikke kan følges og de ansatte kan ha forskjellig måte å utføre oppgavene på. Det følgende er et eksempel:

> Ola og Kari jobber begge som leger ved Nyremedisinsk avdeling. De er autorisert til å slå opp pasientjournalen til alle pasienter som er lagt inn ved denne avdelingen, og har har tilgang til å aktualisere journalene til alle pasientene ved sykehuset. En dag blir Ola bedt om å si sin mening om sykdomsbildet til en pasient som er har time ved Ortopedisk poliklinikk. Han bruker sin aktualiseringsrett til å slå opp denne pasientens journal og lese innholdet. Dette gjør han i et rolig øyeblikk på en ekstra nattevakt han har påtatt seg på grunn av sykdom i avdelingen, et par dager før pasientens avtale. Dette er ikke et brudd på taushetsplikten.
>
> Kari får en dag vite at en nær venninne av henne er innlagt på Avdeling for infeksjonsmedisin. Kari tar kontakt med en kollega som jobber på Infeksjonsmedisinsk, og ber ham fortelle henne hva som er galt med venninnen. Kollegaen nekter, og henviser til taushetsplikten. Kari bruker derfor aktualiseringsrett til å slå opp venninnens journal. Dette er et brudd på taushetsplikten.

I begge eksemplene over kan sporene som blir lagt igjen i tilgangsloggen være misvisende. I det øverste eksemplet vil loggen vise en lege som slår opp journalen til en pasient som ikke er innlagt, og som heller ikke har time ved hans avdeling. Oppslaget blir i tillegg gjort midt på natten, på et tidspunkt hvor legen etter turnussystemet egentlig ikke skulle vært på jobb. Ved en loggjennomgang vil dette journaloppslaget kunne se ut som et ulovlig oppslag. I det andre eksempelet slår en sykepleier opp journalen til en pasient som er innlagt på hennes avdeling mens hun er på vakt. For den som gjennomgår loggen vil det være vanskelig å oppfatte dette som noe annet enn lovlig tilgang, selv om oppslaget egentlig ikke er lovlig.

5.4 Analysestrategier

Det finnes forskjellige strategier for å følge opp logger. Manuell kontroll av logger gjøres ved mange norske sykehus i dag.[31] Det vil si at man tar ut en logg fra en pasients journal og går igjennom den for å kontrollere om det er gjort uberettigede oppslag, enten som et ledd i sykehusets loggoppfølgingsrutine, eller på grunnlag av en konkret mistanke.

Det har vært gjort forsøk på å utvikle systemer for såkalt regelbasert automatisk kontroll av logger ved norske sykehus. Slike datasystemer analyserer oppslagene som er loggført ut fra et forhåndsdefinert sett regler.

5.4.1 Manuell kontroll

Den tradisjonelle måten å kontrollere logger på er manuell. Personell på sykehuset går igjennom loggene fra journalsystemet og sjekker om noen har gjort uberettigede oppslag på pasientjournaler. Den som skal gjennomgå loggen kan velge mellom tre fremgangsmåter. Den første går ut på å undersøke omstendighetene rundt hvert eneste oppslag til man har funnet hjemmelsgrunnlaget for oppslaget. Den andre fremgangsmåten er å gjøre en grovsortering i utgangspunktet, og bare undersøke en del av oppslagene. Grovsorteringen kan for eksempel gjøres ved at bare loggene over aktualiseringer plukkes ut for gjennomgang eller ved å ta stikkprøver.

Den tredje fremgangsmåten er å følge opp logger bare i saker hvor man har grunn til å tro at det er blitt gjort uberettigede oppslag. Loggjennomgangen kan initieres på grunnlag av melding fra pasienten eller en ansatt.

Uansett hvilken fremgangsmåte som blir valgt, må den som kontrollerer loggene ha tilgang til informasjon som setter han eller henne i stand til å avgjøre om et oppslag er berettiget eller uberettiget.

For å kontrollere oppslaget til Kari i eksempelet foran, kan kontrolløren begynne med å sjekke om Kari var involvert i behandlingen. Siden pasienten ikke var innlagt på Karis avdeling, må kontrolløren vite om pasientens diagnose eller Karis fagkompetanse gjør at Kari allikevel skulle være involvert i behandlingen. Pasientens diagnose kan

[31] Rapport frå tilsyn med informasjonstryggleiken ved pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS ved Helse Bergen HF, Haukeland universitetssjukehus og Rapport fra tilsyn med konfidensialiteten og tilgjengeligheten til elektronisk pasientjournal ved Akershus universitetssykehus HF.

kontrolløren finne ved å sjekke journalen. Informasjon om Karis fagkompetanse finnes i personalsystemet. Loggkontrolløren kan i tillegg sjekke om Kari var på vakt den dagen hun gjorde oppslaget. Informasjon om vakter finnes i turnussystemet.

For oppslag som er gjort mellom avdelinger kan det være aktuelt å ha informasjon om hvilke avdelinger pasienten var innlagt på i løpet av sykehusoppholdet. Helsepersonell kan ha behov for å følge opp en pasient etter at pasienten er flyttet til en annen avdeling. Det kan også være nødvendig å sjekke hvilken type behandling pasienten fikk, og om pasienten på noe tidspunkt lå i narkose, ble tatt bilder av (CT, røntgen, MR), mottok fysioterapi eller traff psykiater, prest, sosionom, jordmor eller fikk annen veiledning eller behandling eller mottok andre tjenester. Alle disse yrkesgruppene kan ha hatt behov for tilgang til journalen i løpet av pasientoppholdet.
For oppslag som er gjort på egen avdeling, trenger loggkontrolløren informasjon om hvem på avdelingen som har vært involvert i pasientbehandlingen. Det inkluderer informasjon om personell som kanskje har tatt på seg en ekstravakt på kort varsel eller personell som vikarierer på avdelingen.
Det finnes også mange tilfeller hvor pasientbehandling ikke er hjemmelen for oppslaget. Helseopplysninger kan utleveres hvis pasienten samtykker.[32] Uten pasientens samykke kan helseopplysninger brukes i forskning[33] og kvalitetssikring[34]. Det kan gis tilgang til pasientjournaler som følge av bestemmelser om meldeplikt eller opplysningsplikt[35] og ved utlevering av opplysninger til NAV[36]. Teknisk personell ved sykehuset kan også ha hjemmel til å slå opp i journalen.[37]
Når det gjelder utlevering av opplysninger fra journal i forbindelse med forskning og kvalitetssikring, må den som skal gjennomføre loggjennomgangen ha mulighet til å sjekke hjemmelsgrunnlaget for oppslaget. Det vil si at sykehuset må ha rutiner på plass som dokumenterer beslutninger om gjennomføring av kvalitetssikring og forskning. Dokumentasjonen må også inneholde informasjon om hvem som skal gjennomføre forskningen eller kvalitetssikringen og hvem som skal hente ut informasjonen fra

[32] Helsepersonelloven § 22 første punktum
[33] Helsepersonelloven § 29 første ledd og helseforskningsloven § 35 første ledd
[34] Helsepersonelloven § 26 første ledd
[35] Helsepersonelloven kapittel 6 og 7
[36] Folketrygdloven § 21-4
[37] Helsepersonelloven § 25 annet ledd

journalsystemet. Noen ganger vil dette være samme person, men ikke alltid. Sannsynligvis vil sykehuset være pålagt å ha disse rutinene på plass i følge internkontrollbestemmelsene i helseregisterloven § 17 og personopplysningsforskriften § 3-1. Helseregisterloven § 17 sier at sykehuset skal "etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven". Denne dokumentasjonen kommer også til nytte overfor pasienter som har bedt om utskrift av loggen fra sin journal. Fordi sykehuset er pålagt ansvaret med å sørge for at det ikke blir gjort uberettigede oppslag i en pasients journal, må det være opp til sykehuset å kunne dokumentere at oppslagene som er gjort har et hjemmelsgrunnlag hvis pasienten spør.

Et spørsmål som oppstår i forbindelse med bestemmelsen om kvalitetssikring i helsepersonelloven § 26 er hvor presis delegeringen av kvalitetssikringsoppgavene må være. Bestemmelsen sier at helsepersonell kan gi opplysninger til virksomhetens ledelse i forbindelse med internkontroll og kvalitetssikring, og at informasjonen så langt som mulig skal "gis uten individualiserende kjennetegn". Ledelsen har anledning til å delegere oppgaven med kvalitetssikring og internkontroll til andre innenfor virksomheten. Det kan gjøres fra sak til sak, eller noen kan ha fått tildelt kvalitetssikring som fast oppgave. Dette gjør at den profesjonsbestemte taushetsplikten i dette tilfellet ligner mer på den forvaltningsmessige taushetsplikten, hvor ansatte i samme virksomhet har anledning til å utveksle opplysninger for å kunne organisere arbeidet hensiktsmessig.[38]

For å oppfylle formålet med tilgangskontrollbestemmelsene i helseregisterloven §§ 13 og 13a og taushetspliktsbestemmelsene i helsepersonelloven, kan delegeringen antakelig ikke være for generell. Det vil si at beslutningen om gjennomføring av kvalitetssikrings- og internkontrollprosjekter må være tatt av noen som har fått delegert myndighet til det, og at prosjektene må være spesifisert slik at det er mulig å kontrollere hjemmelsgrunnlaget i etterkant.

Informasjon som kan fortelle hva som var hjemmelen til et oppslag finnes ikke samlet i ett system på sykehuset. Informasjon om diagnose finnes i journalen. Der skal også som regel eventuelle samtykker til utlevering være notert. Andre systemer som kan

[38] Forvaltningsloven § 13b første ledd nr. 3

inneholde relevant informasjon er arkivsystemet og systemer for helseforskning og kvalitetssikring.Loggkontrolløren har altså et mangfold av systemer å forholde seg til under kontrollen. Det enkleste ville være å spørre den ansatte som har gjort oppslaget, men det kan vise seg å være lite fruktbart. En "snoker" vil neppe innrømme at hun har snoket, og helsepersonell gjør så mange oppslag hver dag at det ikke er grunn til å anta at de husker tilfeller som ikke av en eller annen grunn er spesielle. Det kan også være problematisk i forhold til de ansattes rettigheter dersom de blir utsatt for kontroll som oppfattes som usaklig.

Det største problemet med manuell kontroll av logger er at det er ekstremt tidkrevende. I oktober måned 2010 ble det gjort over en million oppslag i journalsystemet på Rikshospitalet.[39] Å sjekke hvert eneste oppslag er ikke gjennomførbart. Selv om det hadde tatt under ett minutt å sjekke om et oppslag er lovlig eller ulovlig, hadde man trengt over 90 mennesker som satt og sjekket journaler 8 timer pr dag for å klare å komme igjennom loggen i løpet av en måned. Det vil si at sykehuset er avhengig av å ha holdepunkter for å velge ut oppslag som skal sjekkes. Dette gjøres ofte ved å velge å bare kontrollere aktualiseringsloggene.
Tanken bak å bare kontrollere aktualiseringsloggene er at det i teorien skulle være relativt få av dem. Det er også lett å tenke seg at "snokere" ville bruke aktualisering fordi tilgangene da er videre. Men som beskrevet i punkt 5.2 er det ikke alltid aktualisering bare blir brukt i unntakstilfeller. Ved noen sykehus inngår aktualisering som en del av den ordinære pasientbehandlingen. Dette betyr at hvor mye man vektlegger om det er brukt aktualisering eller ikke, må variere avhengig av hvordan sykehuset har organisert tilgangene i journalsystemet. På sykehus med utstrakt bruk av aktualisering, bør det at den tilgangsmekanismen er brukt ikke vektlegges for mye i forhold til andre kriterier. Sykehuset må da finne andre holdepunkter for å plukke ut oppslag som skal analyseres.
Når det gjelder stikkprøver, blir utvelgelsen av logger som skal sjekkes gjort tilfeldig. Da blir det også helt tilfeldig hvilke uberettigede tilganger man klarer å avsløre, hvis noen. Men man kan tilpasse arbeidsmengden til et nivå hvor man klarer å gjennomføre,

[39] Tallet gjelder journalsystemet som deles av Rikshospitalet og Radiumhospitalet. De andre sykehusene som inngår i Oslo universitetssykehus (Aker sykehus og Ullevål sykehus) er ikke med i beregningen. Hvis disse sykehusene var med er det grunn til å tro, basert på antall senger, at tallet minst ville doble seg.

og det at de ansatte vet at det foretas stikkprøver kan ha en viss effekt på antallet uberettigede oppslag som gjøres.
Kontroll som gjennomføres bare ved mistanke om uberettiget tilgang, vil sannsynligvis ha høyere treffprosent enn de andre kontrollstrategiene. Men antallet logger som gjennomgåes vil være lavt i forhold til antallet oppslag, og mange uberettigede oppslag vil aldri bli oppdaget.
Den organisasjonsmessige plasseringen til den som kontrollerer loggen kan ha betydning for resultatet. Jo lenger unna stillingen befinner seg på organisasjonskartet, jo mindre sjanse er det for at vedkommende har tilgang til nødvendig informasjon om pasientbehandlingen. Som en følge av dette vil vedkommende kanskje ha mindre sjanse til å avsløre eventuell sniklesing. På den andre siden kan lokal loggkontroll i avdelingene føre til at uberettigede tilganger kanskje ikke blir fulgt opp i den grad det er nødvendig, enten fordi de som jobber på samme avdeling deler en oppfatning av at enkelte oppslag er ”greie” selv om de ikke nødvendigvis er lovlige, eller at ansatte vegrer seg for å varsle om mulige uberettigede oppslag gjort av nære kolleger.
Et alternativ til å la personalet på sykehuset gjennomgå loggen, er å la pasientene gjøre det. De vil være i stand til å gjenkjenne navn på naboer, familie, venner og andre som kanskje kunne ha interesse av helseopplysningene uten å være involvert i behandlingen. Helseregisterloven § 13 siste ledd sier at pasienten kan få utskrift av tilgangsloggen fra sin egen journal, men sykehuset kan ikke vippe ansvaret for loggkontroll over på pasienten. Det er sykehuset som er databehandlingsansvarlig for helseopplysningene, og det er de som har plikt til å sørge for at lovens krav blir overholdt.
Å la pasientene ta ansvaret for å gå igjennom loggene med tanke på uberettiget tilgang er også problematisk av andre grunner. For det første kan man ikke forvente av gjennomsnittspasienten at de skal være i stand til, eller interessert i, å sette seg inn i de relativt kompliserte reglene om hva som er berettiget og uberettiget tilgang. For det andre vil det være vanskelig å sørge for likebehandling, både for pasienter og ansatte. Pasientenes evne og vilje til å gå igjennom sin egen logg vil variere, og det vil medføre at noen pasienters journaler får bedre oppfølging enn andres, og at noen ansatte blir utsatt for kontroll der hvor andre slipper unna.

5.4.2 Regelbasert automatisk analyse

Det har vært gjennomført noen forsøk med automatisk kontroll av logger for å oppdage uberettigede oppslag. Tanken har vært at man ved å utvikle et logganalysesystem kan erstatte den manuelle kontrollen med en automatisk kontroll foretatt av datamaskiner. Logganalysesystemer er utbredt på andre områder, for eksempel finnes det mange leverandører av analyseprogramvare beregnet på driftslogger fra nettverksutstyr og servere.

I de forsøkene som er gjort på å utvikle et logganalysesystem, har man tatt utgangspunkt i det man har ment har vært kjente kriterier for normal eller uønsket aktivitet. I praksis betyr dette at man definerer et sett kriterier som forteller systemet om oppslaget skal plukkes ut for videre analyse. Fordi det er vanskelig å beskrive menneskelig oppførsel som maskinlesbare regler, må reglene brytes ned til mindre deler for å kunne undersøke dataene bedre. Hvis oppslaget ikke oppfyller noen av kriteriene, vil systemet oppfatte det som ok. Før man kjører loggene gjennom systemet, kan man foreta koblinger mot andre systemer som kan inneholde nyttige data. For eksempel personalsystemet, det pasientadministrative systemet og turnussystemet/vaklister.

Kriteriene logganalysesystemet bruker for utvelgelse kan for eksempel være hyppighetsanalyse (mange oppslag foretatt av én bruker mot mange pasientjournaler i løpet av en begrenset tidsperiode – såkalt journalsurfing), oppslag som er gjort av administrativt personell uten at det er angitt en begrunnelse, oppslag som er gjort når den aktuelle ansatte ikke var på vakt, at det er få unike brukere som gjør oppslag fra en PC som er beregnet på felles bruk og står plassert i et vaktrom eller lignende, brukere som har gjort oppslag i sin egen journal eller oppslag som er gjort på andre ansattes journaler.

Kriteriene brukes til å ta ut rapporter fra analysesystemet. Rapportene må så analyseres igjen for å kunne gi informasjon om eventuelle uberettigede oppslag. Den videre analysen kan enten gjøres manuelt, eller av systemet. Avhengig av det som kommer fram i den videre analysen, kan oppslaget bli ansett som lovlig eller ulovlig.

Et eksempel på en rapport kan være en oversikt over alle oppslag som er gjort på andre ansatte på sykehuset som var utskrevet på oppslagstidspunktet. Rapporten gir mulighet til å følge opp disse tilgangene for å få bekreftet at den som gjorde oppslaget hadde hjemmel for å gjøre det, og at oppslaget ikke ble gjort av ren nysgjerrighet.

Funksjonaliteten til et loggsystem som er organisert på denne måten, er først og fremst å hjelpe sykehuset med grovsortering av logger. Ved å kunne sortere oppslag på bestemte kriterier, og kombinasjoner av kriterier, får man et sted å begynne med loggjennomgangen som ikke er basert på tilfeldigheter (som ved stikkprøvekontroll) eller på meldinger fra ansatte eller pasienter. Rapportene kan rangeres slik at rapportene over oppslag som gir utslag på mange kriterier følges opp først, mens andre rapporter bare brukes til informasjon eller til oppfølging av ansatte generelt.
Problemet med denne typen rapporter er at kriteriene som brukes til å lage rapportene i varierende grad er indikatorer på om oppslaget er uberettiget eller ei. Noen av kriteriene fremstår som indikasjoner på ”uønsket adferd” snarere enn ”uberettigede oppslag”, for eksempel der hvor det er gjort mange oppslag fra få unike brukere fra en felles PC. Et annet eksempel på oppslag som ikke nødvendigvis er uberettigede er der hvor helsepersonell har slått opp sin egen journal. Personvernmessig er dette uproblematisk, men retten til innsyn i egen journal i pasientrettighetsloven § 5-1 er ikke ubetinget. Dersom det er ”påtrengende nødvendig for å hindre fare for liv eller alvorlig helseskade for pasienten selv, eller innsyn er klart utilrådelig av hensyn til personer som står pasienten nær”, kan pasienter nektes innsyn i egen journal. Denne forhåndsvurderingen blir det ikke mulig å foreta der hvor helsepersonell gjør oppslag i sin egen journal. Et annet spørsmål er om helsepersonell har behov for tilgang til sin egen journal, og om oppslaget av den grunn er ulovlig som en følge av helseregisterloven § 13 første ledd annet punktum som sier at tilgangen skal være nødvendig for helsepersonellets arbeid.

Når man definerer kriterier og bestemmer hvilke kriterier eller kombinasjoner av kriterier som skal prioriteres i oppfølgingen, må man vurdere hvor sterk indikasjon oppfyllelse av et kriterium gir på at oppslaget er uberettiget. Det kan for det første være problematisk å utsette ansatte for kontroll basert på et svakt kriterium. For det andre må målet med et logganalysesystem ikke bare være å automatisere loggjennomgangen, men også forbedre og effektivisere den slik at man har sterkere indikasjoner på at ulovlige oppslag er foretatt enn man har ved manuell kontroll.

For å kunne plukke ut de oppslagene som er ulovlige trenger man tilgang til data utover det som finnes i loggen. Hvis man kobler loggene mot andre datasystemer, for eksempel personalsystem, turnussystem, pasientadministrativt system og journalsystemet har man

noe mer informasjon å basere en utvelgelse på. For eksempel når de ansatte hadde vakt, når pasienten var innlagt og hvilken avdeling han var innlagt på og om pasienten har avgitt samtykke til utlevering av informasjon. Men data som ligger i disse systemene sier i utgangspunktet ingenting om hvilke pasientjournaler den ansatte har lovlig tilgang til.

Der hvor hjemmelsgrunnlaget ikke er pasientbehandling, trenger loggkontrolløren informasjon som gjør henne i stand til å finne hjemmelsgrunnlaget. Det kan for eksempel være forskningsstudier og kvalitetssikring (se forøvrig punkt 5.4.1 om manuell kontroll). Dette er informasjon som ofte ikke finnes samlet i ett system. Få sykehus har et samtykkeregister hvor samtykker fra pasienten til forsknings- og/eller kvalitetsstudier er registrert. De enkelte forskningsprosjektene har en oversikt over hvilke pasienter som er inkudert i studien, men i elektronisk form er denne informasjonen ofte avidentifisert. På grunn av at dataene ofte ikke finnes lett tilgjengelig for integrasjon mot et logganalysesystem, vil logganalysesystemet måtte plukke ut oppslag som synes å mangle hjemmel i helsebehandling uten å kunne sjekke om det finnes andre hjemler for oppslag. Denne jobben må da gjøres manuelt.

Et av målene med å finne nye metoder for logganalyse er å redusere antallet oppslag med usikkert hjemmelsgrunnlag så mye som mulig slik at man både sparer ressurser, og sparer de ansatte for unødig kontroll og mistanke.

5.4.3 Mønstergjenkjenning

Kort fortalt går mønstergjenkjenning ut på å lete etter mønster i data.

Mønstergjenkjenning er en strategi som er spesielt godt egnet der hvor datamengden er så stor at manuell analyse er umulig, eller det er vanskelig å finne egenskaper som gjelder for alle dataene, og som entydig beskriver det man er ute etter å finne.

5.4.3.1 Hvordan lete etter mønstre i data?

I 2009 ble det gjennomført en pilot for å teste mønstergjenkjenning som strategi for analyse av tilgangslogger fra det elektroniske pasientjournalsystemet på Ullevål sykehus. Piloten ble gjort i samarbeid med SAS Institute, og metoden som ble brukt i piloten er beskrevet nedenfor. Beskrivelsen er hentet fra sluttrapporten fra prosjektet[40]

[40] Mønstergjenkjenning for å avsløre misbruk av tekniske tilganger. Sluttrapport fra pilot ved Oslo universitetssykehus – Ullevål" (Inge Krogstad, SAS Institute, Oslo, august 2009)

og sluttrapporten fra Fagruppen Mønstergjenkjenning[41] som gjennomførte møter våren 2010.

Fremgangsmåten ved mønstergjenkjenning er på mange måter det motsatte av fremgangsmåten ved manuell kontroll eller regelbasert automatisk kontroll. I stedet for å prøve å finne egenskaper ved oppslag som gjør at man kan si at de er uberettigede, prøver man ved hjelp av mønstergjenkjenning å definere uberettigede oppslag negativt. Det vil si at man prøver å finne ut hva som er "normal" bruk av journal for et individ eller en gruppe, og så behandle avvik fra dette som mulige uberettigede oppslag. Utover dette benytter man noen av de samme mekanismene ved mønstergjenkjenning som ved de andre analysestrategiene, blant annet kobling mot turnuslister.

Prosessen kan lettest forklares ved å bruke det samme eksempelet som i punkt 5.3.2. Ved hjelp av mønstergjenkjenning kan disse to oppslagene analyseres. Først brukes en metode som heter statistisk analyse til å kartlegge Nyremedisinsk avdelings oppslagsmønster. Det gjøres ved å analysere en samlet logg over alle oppslag ansatte på Nyremedisinsk har gjort over en viss tid. Den analysemodellen som brukes kalles clustering. Clustering går ut på å dele en heterogen gruppe oppslag inn i en rekke mindre, mer homogene grupper. Clustering er et eksempel på ikke-ledet læring, noe som vil si at man ikke kjenner gruppenes egenskaper eller antallet grupper på forhånd. Analysemodellen finner gruppene etterhvert som den går igjennom oppslagene, og hvert oppslag vil bli klassifisert som tilhørende en gruppe modellen allerede har funnet, eller en ny gruppe. Hvilke egenskaper ved oppslagene modellen skal tillegge mest vekt ved sorteringen kan bestemmes på forhånd, og kan justeres etterhvert. Vi vet for eksempel at noen avdelinger på sykehuset samarbeider mer enn andre. I dette samarbeidet kan de ansatte ved en avdeling ha bruk for å aktualisere pasienter ved den avdelingen de samarbeider med. Vi kan finne ut hvilke avdelinger det er, hvem som oftest gjør oppslagene og når de gjør dem ved å bruke clustering til å gruppere oppslagene.

I vårt eksempel har Nyremedisinsk avdeling oftest behov for å gjøre oppslag mot Ortopedisk avdeling, Infeksjonsmedisinsk avdeling, Barneklinikken og Avdeling for blodsykdommer. På grunnlag av samme analysen kan vi også vite hvilke diagnoser de ansatte ved Nyremedisinsk oftest gjør oppslag på, hvilke aktiviteter de utfører i

[41] Sluttrapport Fagruppen Mønstergjenkjenning Fase 1" (Sekretariatet ved SAS Institute, Oslo, oktober 2010. Inge Krogsrad – sekretær for faggruppen)

journalen (for eksempel lese eller skrive) og når på døgnet de som regel gjør oppslag.
Etter at clusteranalysen er utført, gjøres en annen type analyse som kalles assosiasjonsanalyse. Det er en metode for å oppdage sammenhenger mellom forskjellige egenskaper. I varehandelindustrien brukes for eksempel assosiasjonsanalyse ofte til å gi kunder anbefalinger om produkter de kanskje kan være interessert i. Metoden ser på hva kunden kjøper og har kjøpt før, og anbefaler produkter på grunnlag av hva andre kunder med lignende kjøpemønster har kjøpt. I vårt tilfelle brukes assosiasjonsanalyse til å finne ut hvor vanlig det er at forskjellige egenskaper ved et oppslag opptrer sammen. Vi vet allerede at ansatte på Nyremedisinsk aktualiserer mye mot Avdeling for infeksjonsmedisin. Men hvor vanlig er det at de aktualiserer pasienter på Avdeling for infeksjonsmedisin med diagnosen syfilis (som er Karis venninnes diagnose)? Og hvor vanlig er det at Kari gjør det? Er det så vanlig at det er grunn til å si at det er normal bruk?
Resultatene fra assosiasjonsanalysen brukes til å bygge såkalte hvitelister. Hvitelister er lister over sammenhenger mellom egenskaper ved ett oppslag, for eksempel en ansatts organisasjonstilhørighet og rolle og en pasients diagnose. Sammenhengene på hvitelisten er definert som normale.
Hvitelistene er grunnlaget for det som kalles scenarier. Et scenario er en hendelse beskrevet som et sett parametre. Hvert scenario kan være basert på en eller flere hvitelister som beskriver hva som er ”normale” sammenhenger.
For eksempel hvis vi sammenligner oppslaget til Kari med scenariet ”Oppslag som ikke er relevant for pasientforløp”, får vi følgende resultat:

- Ansatts rolle: Lege
- Ansatts avdeling: Avdeling for nyremedisin
- Pasients avdeling: Infeksjonsmedisinsk avdeling
- Pasients diagnose: Syfilis
- Tilgangstype: Aktualisering
- Aktivitet: Lese journal
- Tidspunkt for oppslag: 01.01.2011 12.41

Hver parameter i scenariet brukes til å bestemme oppslagets risikoscore. Man kan bestemme hvor mye hver parameter i et scenario skal telle for resultatet. I vårt eksempel

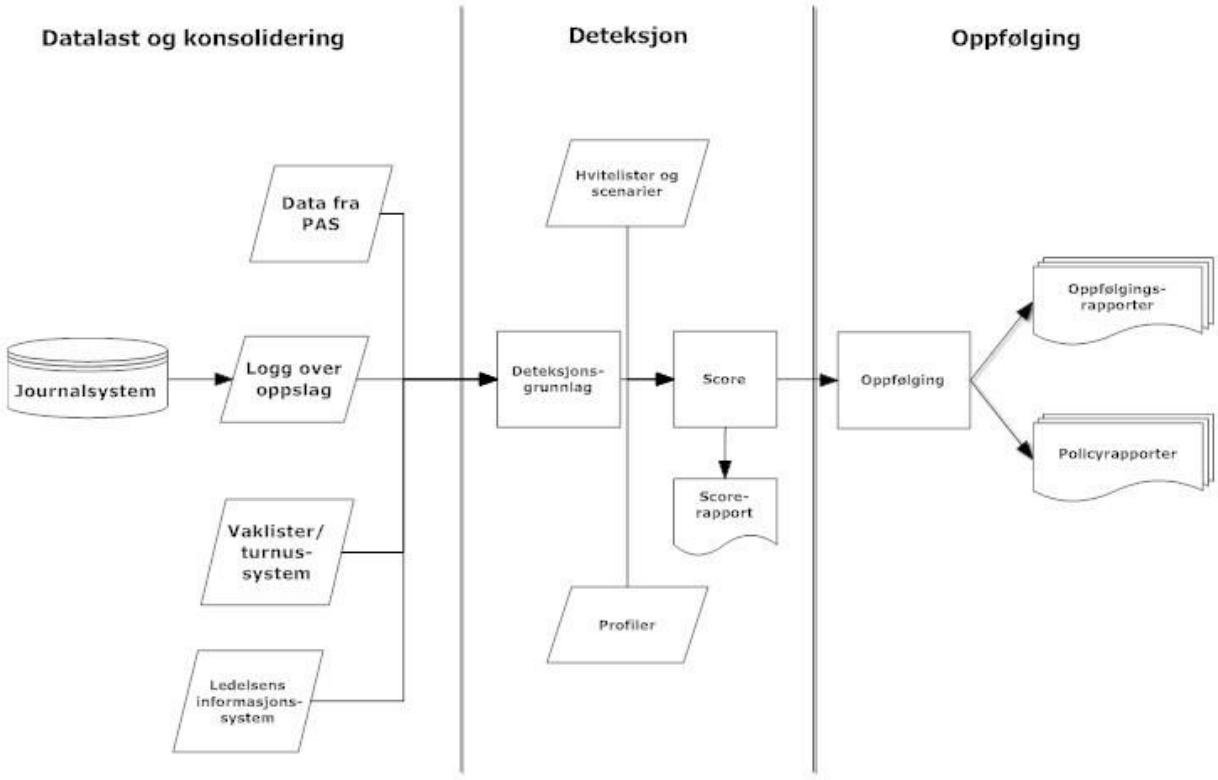
antar vi at parametrene ansatts avdeling, pasients avdeling og pasients diagnose er de som vil fortelle oss mest om oppslaget er relevant for pasientforløpet eller ei. Derfor blir de vektet tyngst. Hvitelistene forteller oss at oppslag fra Nyremedisinsk til Infeksjonsmedisinsk er vanlige, så parametrene ”ansatts avdeling” og ”pasients avdeling” er ikke risikofaktorer. Hvis vi går ut i fra at vi vet fra hvitelistene at oppslag fra Nyremedisinsk mot en pasient med diagnosen syfilis ikke er vanlig, bidrar parameteret ”pasients diagnose” til å øke scenariets risikoscore. Vi kan også tenke oss at vi har en sammenheng som sier at når Nyremedisinsk slår opp journalen til en pasient ved Infeksjonsmedisinsk vil det som regel være for å dokumentere behandling, altså skrive i journalen. I vårt tilfelle leser Kari journalen til venninnen. Derfor kan også parameteren ”aktivitet” være en risikofaktor i dette scenariet.

I Oles tilfelle kan man tenke seg at verken pasientens avdeling, pasientens diagnose eller Oles aktivitet i journalen er risikofaktorer. Da vil den eneste risikofaktoren som gjenstår være tidspunkt for oppslag. Dette vil gi Oles scenario en lavere risikoscore enn Karis.

Andre eksempler på scenarier kan være oppslag som ikke er relevante for rollen (for eksempel hvor en arkivansatt leser en journal i stedet for å skanne inn et dokument), oppslag på tvers av fagområde (for eksempel en kirurg slår opp på en pasient som ikke har fått kirurgisk behandling) eller oppslag på kolleger.

Resultatet av analysen er en liste over oppslag som har fått en risikoscore. Sykehuset kan på grunnlag av risikoscoren bestemme hvilke oppslag som skal følges opp videre, og prioritere dem slik at de tilsynelatende alvorligste bruddene på taushetsplikten kan følges opp først.

Figuren under beskriver oppsettet i piloten:



Figur 1: Oppsett av deteksjonsprosess i piloten[42]

Prosessen kan deles inn i tre hovedfaser:

1) Datalast og konsolidering
   I denne fasen klargjøres data for analyse. Data fra andre aktuelle systemer enn det elektroniske pasientjournalsystemet innhentes, og dataene vaskes (det vil si at uinteressant informasjon fjernes, og datatypene standardiseres slik at de er de samme i alle kildedataene).

2) Deteksjon
   I denne fasen kjøres dataene gjennom scenariene. Hvert oppslag risikoscores.

3) Oppfølging
   Rapportene som blir generert av deteksjonsprosessen brukes som underlag for å videre undersøke oppslag.

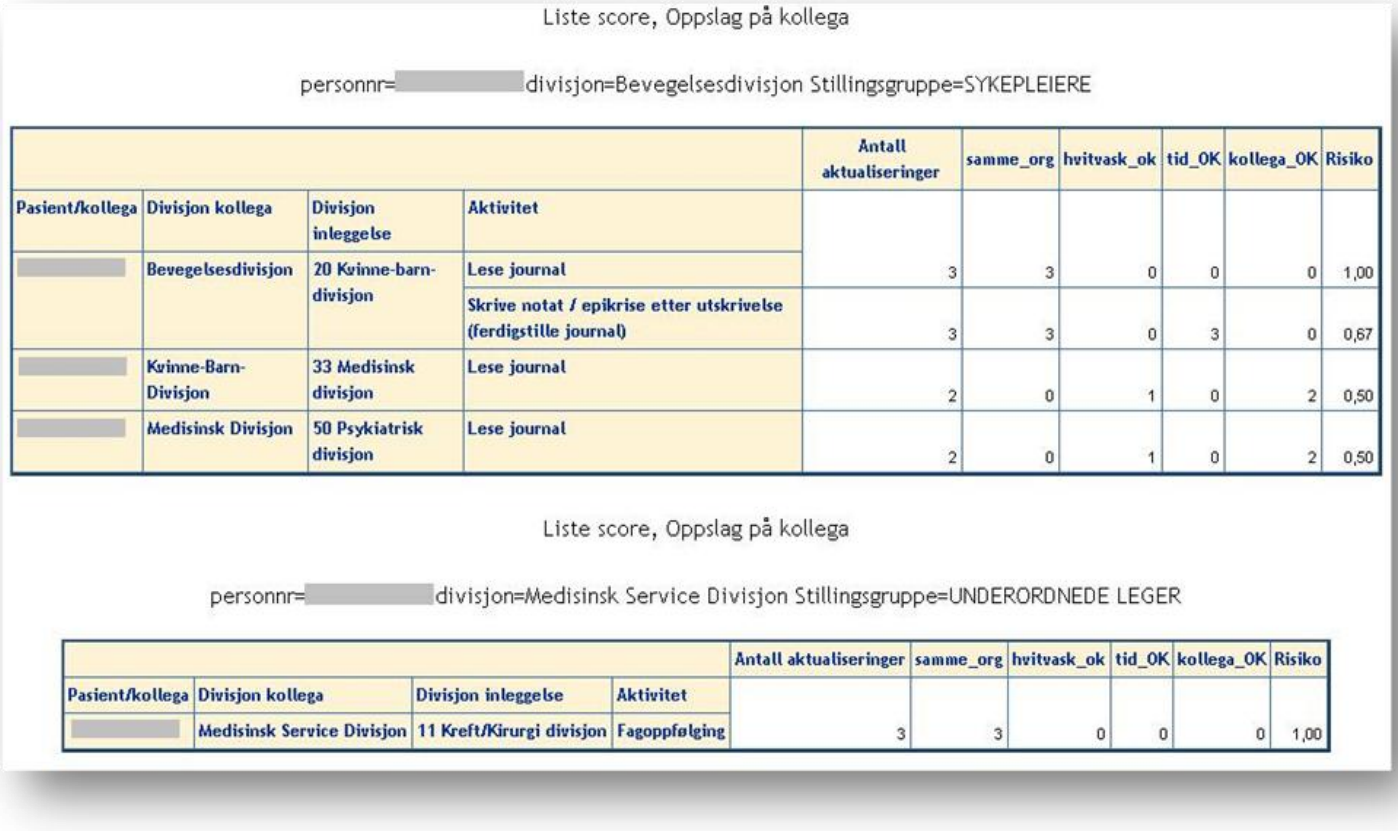
5.4.3.2 Resultatene av piloten på Oslo universitetssykehus – Ullevål

Metodikken beskrevet ovenfor ble testet på pilotdata hentet fra Ullevål sykehus' systemer. Pilotdataene bestod blant annet av aktualiseringslogger fra det elektroniske journalsystemet. Resultatene av testingen indikerte at det var grunn til å operere med tre arbeidshypoteser:

[42] Mønstergjenkjenning for å avsløre misbruk av tekniske tilganger. Sluttrapport fra pilot ved Oslo universitetssykehus – Ullevål s. 11

- Det gjennomføres aktualisering som ikke er relevant for pasientforløpet
- Det gjennomføres aktualisering som ikke er relevant for rollen
- Det gjennomføres aktualisering på kolleger som ikke er relevant for behandling og/eller diagnose

Med utgangspunkt i arbeidshypotesen ”det gjennomføres aktualisering på kolleger som ikke er relevant for behandling og/eller diagnose” ble det utarbeidet et scenario for dette. Loggene ble kjørt gjennom scenarioet designet for arbeidshypotesen, og det ble utarbeidet flere typer rapporter i etterkant av kjøringen. Rapporten under viser en liste over oppslag med risikoscore og en oversikt over hvilket parameter som ga utslag på risikoscoren.



Liste score, Oppslag på kollega

personnr= divisjon=Bevegelsesdivisjon Stillingsgruppe=SYKEPLEIERE

				Antall aktualiseringer	samme_org	hvitvask_ok	tid_OK	kollega_OK	Risiko
Pasient/kollega	Divisjon kollega	Divisjon inleggelse	Aktivitet						
	Bevegelsesdivisjon	20 Kvinne-barn-divisjon	Lese journal	3	3	0	0	0	1,00
			Skrive notat / epikrise etter utskrivelse (ferdigstille journal)	3	3	0	3	0	0,67
	Kvinne-Barn-Divisjon	33 Medisinsk divisjon	Lese journal	2	0	1	0	2	0,50
	Medisinsk Divisjon	50 Psykiatrisk divisjon	Lese journal	2	0	1	0	2	0,50

Liste score, Oppslag på kollega

personnr= divisjon=Medisinsk Service Divisjon Stillingsgruppe=UNDERORDNEDE LEGER

				Antall aktualiseringer	samme_org	hvitvask_ok	tid_OK	kollega_OK	Risiko
Pasient/kollega	Divisjon kollega	Divisjon inleggelse	Aktivitet						
	Medisinsk Service Divisjon	11 Kreft/Kirurgi divisjon	Fagoppfølging	3	3	0	0	0	1,00

Figur 2: Eksempel på rapport fra piloten[43]

[43] Ibid.

Målsetningen med rapportene er først og fremst å gi ledelsen et verktøy for å håndtere mulige uberettigede oppslag.

5.4.3.3 Justering av parametre og vekting

Et viktig arbeid som må gjøres for å unngå feil i analyserapportene er å justere parametrene som brukes i scenarier og vektingen av dem. Når man tester metodene er det viktig at man gjør oppfølging for å finne ut om de oppslagene som får høy risikoscore virkelig er uberettigede. Hvis metoden gir treff på oppslag som er berettigede, men opptrer så sjelden at de framstår som et avvik i datamateriale, må parametre og vekting justeres slik at man ikke får treff på denne typen oppslag igjen. Dette stiller krav til organisasjonen rundt systemet. Man må ha prosedyrer og personell som er dedikert til å følge opp systemet i den grad det er nødvendig. Behovet for justering av parametrene og vektingen vil være størst i begynnelsen, og vil avta etterhvert som metodene blir finjusterte. Men man må allikevel regne med å drive noe justering så lenge systemet er i bruk.

6 Oppfølging av analysen

Uansett om sykehusene velger å ha manuell loggkontroll, regelbasert automatisk analyse av logger eller logganalyse basert på mønstergjenkjenning, må de ha rutiner for oppfølging av analyseresultatene. Hva slags oppfølging som kreves kan variere avhengig av hvilken metode for logganalyse som er valgt.

Ved manuell kontroll av logger vil resultatet av kontrollen være en liste over oppslag man ikke finner hjemmelsgrunnlag for. Oppfølgingen vil hovedsaklig dreie seg om å følge opp disse oppslagene til man får avklart om den ansatte hadde hjemmel for å gjøre det eller ei.

Hvis sykehuset bruker regelbasert automatisk analyse, vil rapportene inneholde oppslag som har gitt utslag på kriterier som skal definere uberettigede oppslag. Selv om kriteriene kan være mer eller mindre treffende, vil resultatet være en liste over oppslag som på en eller annen måte representerer uønsket oppførsel slik som sykehuset har definert det. For å få en effektiv oppfølging av resultatene, må sykehuset ta stilling til

hvordan de ønsker å følge opp oppslagene basert på hvilke kriterier som har gitt utslag. Det er ikke sikkert at det er ønskelig å følge opp oppslag som er gjort på den ansattes egen journal på samme måte som oppslag som oppfyller kriteriene for journalsurfing. Oppfølgingen av resultater fra mønstergjenkjenningsanalyse kan ha flere forskjellige aspekter. For det første gir rapportene mulighet for å håndtere de åpenbare taushetspliktbruddene. Risikoscoren hvert oppslag får gir grunnlag for å si hvilke oppslag som bør prioriteres. For det andre gir rapportene grunnlag for å si noe om hvor ofte og i hvilket omfang uberettigede oppslag foregår. Denne informasjonen kan brukes til å rette informasjons- og opplæringstiltak mot de ansatte slik at man unngår uberettigede oppslag som et resultat av uvitenhet. For det tredje kan kunnskapen om hvordan de ansatte bruker det elektroniske journalsystemet brukes til å lage nye tilgangsmekanismer, slik at man kan redusere problemet med at ansatte har tilganger til flere journaler enn de trenger.

6.1 Feiltoleranse ved logganalyse

Ved logganalyse oppstår spørsmålet om hvor stor feiltoleranse systemet kan ha. Hovedårsakene til feilklassifikasjoner er svake kriterier for utvelgelse av oppslag og dårlig kvalitet på kildedata. Problemet med svake kriterier gjelder særlig manuell kontroll og regelbasert automatisk analyse. Dårlig kvalitet på kildedata er hovedsaklig et problem for de to automatiserte strategiene. Uavhengig av hvilken analysestrategi man velger, vil oppfølgingen av analyseresultatene måtte ta hensyn til eventuelle feilklassifikasjoner.

6.1.1 Kildedata

Ved logganalyse kan sykehuset velge å hente inn opplysninger fra flere forskjellige kildesystemer. Det pasientadministrative systemet (PAS) og flere andre systemer inneholder informasjon om pasientene. Informasjon om de ansatte finnes blant annet i den elektroniske brukerkatalogen (som er en katalog over alle brukernavn og hvilke roller og rettigheter som er knyttet til disse) og i personalsystemet og/eller turnussystemet. Avhengig av hvilke resultater man håper på å oppnå med logganalyse, kan det være naturlig å hente opplysninger fra ett eller flere av disse. Det avgjørende ved valget av hvilke systemer sykehuset skal hente data fra, bør være hvilken nytteverdi sykehuset ser for seg at dataene har. Hvis sykehuset velger å ha med data som har liten

eller ingen nytteverdi fordi det kan være ”kjekt å ha”, kan resultatet bli at analyseresultatene får dårligere treffsikkerhet fordi irrelevante data er lagt til grunn.

Å velge å hente inn data fra flere forskjellige kildesystemer kan føre til at det behandles flere personopplysninger ved automatisk analyse enn ved manuell kontroll, både om pasienter og ansatte. Det er i utgangspunktet ikke et problem så lenge dataene er nyttige. Imidlertid er det et grunnleggende prinsipp innenfor personvern at det ikke skal samles inn flere personopplysninger enn det som er nødvendig for å oppfylle formålet med behandlingen av personopplysninger (minimalitetsprinsippet).[44] Prinsippet finnes i EUs personverndirektiv art 6 første ledd bokstav c, som sier at opplysningene skal være ”adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”.[45] Prinsippet er ikke åpenbart i norsk lovgivning, men personopplysningsloven § 11 første ledd bokstav d sier at opplysningene skal være ”tilstrekkelige og relevante for formålet ved behandlingen”. Justis- og politidepartementet skriver i forarbeidene til personopplysningsloven at ”Uttrykket "relevante" markerer en ytre grense for hvilke personopplysninger som kan trekkes inn i behandlingen; behandlingen må ikke omfatte unødvendige personopplysninger”[46]. Hvis sykehuset vurderer å hente data som bare har minimal nytte for logganalysen, må sykehuset vurdere forholdet til relevansbegrensningen i personopplysningsloven § 11.

6.1.2 Datakvalitet

For at en loggkontroll skal være vellykket, er sykehuset avhengig av god kvalitet og struktur på kildedata, inkludert selve loggene. Dette vil si at dataene må være korrekte, og at riktig informasjon må ligge i riktig felt. For eksempel må rettigheter og roller i det elektroniske journalsystemet stemme med de rettigheter og roller som den samme brukeren har i den elektroniske brukerkatalogen og hvilken rolle vedkommende faktisk har i sitt daglige arbeid. Eventuelle feilkilder må elimineres så godt som mulig. Hvis ansatte for eksempel har for vane å bytte vakter seg i mellom uten å oppdatere turnussystemet, må sykehuset sørge for at de ansatte registrerer endringer i turnussystemet. Data må også kunne hentes ut fra systemene på en måte som sørger for

[44] Se Bygrave (2002) s. 59-60 om minimalitetsprinsippet.
[45] EP/Rdir 95/46/EF
[46] Ot.prp. nr. 92 (1998-99) kapittel 16, merknadene til § 11

at dataenes integritet er ivaretatt.
Mønstergjenkjenning er i større grad enn de andre analysestrategiene avhengig av at kvaliteten på selve loggene er god, ettersom analyseresultatene er basert på bruksmønstre som er funnet ved analyse av logger.
Sykehuset er etter personopplysningsloven § 14 forpliktet til å ha tiltak på plass som sørger for tilfredsstillende kvalitet på personopplysninger. Innføring av et automatisk logganalysesystem kan i visse tilfeller skjerpe kriteriene for hva som er tilfredsstillende datakvalitet.

6.1.3 Feilklassifikasjoner

En av kildene til feil i kildedata og dårlig datakvalitet er ansatte som er logget på med en annen ansatts brukernavn og passord. For å kunne bruke analysesystemet til å følge opp uberettigede oppslag, er man avhengig av å ha en entydig kobling mellom en ansatt og dennes brukerkonto (brukernavn og passord). Denne koblingen er ikke alltid sikker fordi det hender at en ansatt oppgir brukernavnet og passordet sitt til en annen ansatt, eller fordi en ansatt ikke logger ut av journalsystemet etter å ha brukt det, og nestemann som kommer til PCen bruker samme påloggingen.
I en spørreundersøkelse gjennomført på anestesiavdelingen på Stavanger universitetssykehus svarer 29% av de ansatte at de daglig går forbi en PC hvor journalsystemet er logget på, og 42% svarer at det skjer ukentlig.[47] Selv om man går ut i fra at situasjonen ved Stavanger universitetssykehus ikke uten videre kan overføres til andre sykehus, gir dette en indikasjon på at man ikke uten videre kan gå ut i fra at en ansatt alltid er autentisert med sin egen bruker i journalsystemet.
Brukernavn og passords konfidensialitet er ikke direkte nevnt i lovverket, men bestemmelsene forutsetter at brukere skal kunne identifiseres på grunnlag av brukernavn og passord. For eksempel skal tilganger tildeles på individuell basis i følge helseregisterloven § 13.
At brukere deler brukernavn og passord mellom seg er også i strid med grunnleggende sikkerhetspraksis. Praksisen er ikke tillatt i henhold til Norm for informasjonssikkerhet, som er et sett med krav til informasjonssikkerhet som stilles til sykehus som er

[47] Er vi egentlig så sikre? Gro Anita Fosse [et.al]. s. 39.

tilknyttet Norsk Helsenett.[48] Normen stiller krav om at autentiseringen skal sikre at rett person autentiseres. [49] Norsk Standard NS-ISO/IEC 27002:2005 som heller ikke er bindende, men som er en anerkjent global informasjonssikkerhetsstandard utarbeidet av ISO, sier at brukere bør signere et dokument som forplikter dem til å holde passordet sitt hemmelig.[50] Sykehus kan også i interne sikkerhetsinstrukser eller arbeidskontrakter pålegge de ansatte å ikke dele passordet sitt med andre. Det er viktig at sykehuset avklarer på forhånd hvilket ansvar de ansatte skal ha for oppslag som er gjort med deres brukernavn og passord.

Andre problemområder er fellesbrukere (brukernavn og passord som identifiserer en gruppe ansatte i stedet for en enkelt ansatt) og dårlig kontroll med brukerkontoene til ansatte som har sluttet eller er i permisjon. Bruk av fellesbrukere nevnes ikke spesifikt i helseregisterloven eller personopplysningsforskriften, men bruken av dem er i strid med Norm for informasjonssikkerhet i helsesektoren som sier at "Flere personer skal ikke benytte samme autentiseringskriteria".[51] ISO 27002 tillater bruken av fellesbrukere, men bare i den utstrekning det er nødvendig, og bare der hvor det er godkjent og dokumentert.[52] Hvorvidt sykehusene i noen grad kan tillate fellesbrukere vil avhenge av de konkrete informasjonssikkerhetsvurderingene som gjøres. Men det er grunn til å utvise forsiktighet ved oppretting av fellesbrukere ettersom de kan redusere sporbarheten betraktelig.

Både Norm for informasjonssikkerhet og ISO 27002 sier at brukerkontoer som ikke er i bruk skal sperres.[53]

To typer feilklassifikasjoner som oppstår ved automatisk logganalyse er falske positive og falske negative. En falsk positiv er et oppslag som er berettiget, men som allikevel blir plukket ut av systemet som et mulig uberettiget oppslag. En falsk negativ er et oppslag som er uberettiget, men som ikke blir klassifisert som dette av analysesystemet. Det er flere forhold ved kontroll av logger som gjør at man får falske positive og negative. For regelbasert automatisk analyse er det største problemet å definere kriterier

[48] Norm for informasjonssikkerhet i helsesektoren s. 21
[49] Norm for informasjonssikkerhet faktaark 15 s. 1
[50] NS-ISO/IEC 27002:2005 s. 62
[51] Norm for informasjonssikkerhet i helsesektoren s. 21
[52] NS-ISO/IEC 27002:2005 s. 61
[53] NS-ISO/IEC 27002:2005 s. 61, Norm for informasjonssikkerhet faktaark 14 s. 4

for hvilke oppslag som er uberettigede. Det finnes ikke ett kriterium, eller ett sett kriterier, som definerer et ulovlig oppslag. Man kan prøve å finjustere kriteriene så mye som mulig, men det er store variasjoner i behovet for oppslag i pasientjournalen. Hvilke typer helsepersonell som har tilgang, hvor mange som har tilgang, hvordan helsepersonellet velger å gjennomføre oppgavene, rimelig antall oppslag i forhold til oppgavene, pasientens diagnose og behov for behandling og tilleggsbehov knyttet til for eksempel kvalitetssikring er variable som forandrer seg fra pasient til pasient og fra avdeling til avdeling. Men hovedkriteriet for at tilgangen skal være berettiget vil hele tiden være det samme, nemlig at personellet er involvert i behandlingen eller har annen hjemmel.

Det finnes flere måter å takle problemene med falske positive og negative på. Sykehuset kan velge å prøve å unngå falske positive ved å definere kriteriene så strengt som mulig. Da vil de bare få rapporter over oppslag hvor det er rimelig sikkert at oppslaget er uberettiget, for eksempel fordi det gir utslag på et kriterium som ikke gir så mye tolkningsrom (oppslag i egen journal) eller fordi oppslaget har gitt utslag på mange forskjellige kriterier eller scenarier. Ved å velge denne fremgangsmåten kan sykehuset eliminere de fleste falske positive, men det vil til gjengjeld stå igjen med en del falske negative fordi systemet ikke oppdager de uberettigede oppslagene som ikke møter kriteriene. Avhengig av målsetningen, kan dette gjøre systemet ineffektivt i større eller mindre grad.

En annen fremgangsmåte er å legge seg på den strenge linje, og undersøke alle oppslag som tilfredsstiller ett eller ett sett kriterier eller scenarier som er definert for ulovlige oppslag. Dette vil mest sannsynlig føre til en høy andel av falske positive, men systemet vil samtidig også få med seg de fleste uberettigede oppslagene.

Målet med enhver automatisk analyse er å finne en metode som er så veldefinert at den eliminerer de fleste falske positive og negative. For å få til det må sykehuset finne en balanse hvor kriteriene er strenge nok, men ikke for strenge.

Hvor stor feiltoleranse et logganalysesystem kan ha, vil avhenge av målsetningen med logganalysen og systemets effektivitet i forhold til de andre alternativene man har for logganalyse. Dersom sykehuset har et logganalysesystem som er relativt effektivt, og som hjelper det med å avdekke flere uberettigede oppslag enn ved for eksempel manuell kontroll, vil noen feilklassifikasjoner kunne tolereres. Sykehuset bør være klar over muligheten for at det vil finnes feilklassifikasjoner i rapportene, og ha rutiner for å

håndtere dem og sjekke dem ut på et så tidlig tidspunkt som mulig. Arbeidet med å sortere ut feilklassifikasjoner kan kreve mye ressurser, og et høyt antall feilklassifikasjoner kan være problematisk i forhold til saklighetskravet i aml. § 9-1[54]. For mange feil kan i verste fall sparke bena under et logganalysesystem fordi systemet ikke er til å stole på, og skaper merarbeid for alle involverte parter. Ikke minst for de ansatte som kanskje vil føle at de må forsvare seg mot anklager som ikke er basert på fakta.

Situasjonen er anderledes for falske negative enn for andre feilklassifikasjoner ettersom falske negative aldri vil dukke opp i rapporter. Hvis sykehuset mistenker at de har et logganalysesystem som resulterer i at en del uberettigede oppslag aldri blir oppdaget, må de gjøre en vurdering på om nytteeffekten av logganalysesystemet er så stor at de falske negative kan tolereres.

Spørsmålet om feiltoleranse har også betydning for bevisstyrken til analyseresultatene. Jo høyere feiltoleranse sykehuset opererer med, jo lavere vil bevisstyrken til analyseresultataene være. Dette må få konsekvenser for oppfølgingen.

For regelbasert automatisk analyse vil dette bety at dersom utvelgelseskriteriene bare er svake indikatorer på at det har blitt foretatt et ulovlig oppslag, må dette reflekteres i måten analyseresultatene følges opp på. Det vil da være nødvendig med ytterligere kontroller lik de som gjøres ved manuell kontroll før man kan konkludere med at et oppslag er uberettiget.

Mønstergjenkjenning skiller seg fra manuell kontroll og regelbasert automatisk analyse med hensyn til bevisspørsmålet. Der manuell kontroll og regelbasert automatisk analyse går ut på lete etter oppslag som er ulovlige ved å finne egenskaper som beskriver disse, leter mønstergjenkjenning etter egenskaper som beskriver lovlige oppslag. Det vil si at når man sitter med analyseresultater etter manuell kontroll og regelbasert automatisk analyse, vil etterkontrollen være basert på en antakelse om at det finnes bevis på at oppslaget er uberettiget. Oppfølgingen av resultatene etter mønstergjenkjenning vil være basert på et fravær av bevis for at oppslaget er berettiget. Fravær av bevis for en ting, er ikke alltid et bevis for det motsatte. Dette må sykehuset ta hensyn til ved oppfølgingen. Det kan være nødvendig å justere parametre og vekting for å få bedre

[54] Se Ot.prp. nr. 49 (2004-2005) s. 145 om nøyaktighet i de resultater som kontrollen avstedkommer

treff, og det kan være nødvendig med etterfølgende kontroller. Ved effektiv justering av parametre og vekting vil behovet for etterfølgende kontroller etterhvert bli mindre.

6.1.4 Automatisert oppfølging

Hvis sykehuset tar i bruk regelbasert automatisk analyse eller mønstergjenkjenning for logganalyse, legger personopplysningsloven § 22 begrensninger på i hvilken grad oppfølgingen av logganalysen kan være automatisert. Bestemmelsen sier at hvis en avgjørelse "har rettslig eller annen vesentlig betydning for den registrerte og fullt ut er basert på automatisk behandling av personopplysninger, kan den registrerte som avgjørelsen retter seg mot, kreve at den behandlingsansvarlige gjør rede for regelinnholdet i datamaskinprogrammene som ligger til grunn for avgjørelsen". At avgjørelsen "fullt ut" må være basert på automatisk behandling av personopplysninger vil si at det ikke må ha skjedd noen individuell vurdering av saken, og at både innsamling av opplysninger og behandlingen av opplysningene må være "uberørt av menneskehender".[55]

Ved en fullt ut automatisert avgjørelse har den ansatte rett til å kreve at avgjørelsen overprøves av en fysisk person, med mindre "den registrertes personverninteresser ivaretas på tilstrekkelig måte og avgjørelsen er hjemlet i lov eller knytter seg til oppfyllelse av kontrakt", jf. personopplysningsloven § 25. At den registrertes personverninteresser skal være ivaretatt innebærer blant annet at det skal være gitt klageadgang og begrunnelse.[56]

Hvis sykehuset velger å automatisere oppfølgingen av logganalysen, må de altså utlevere informasjon for eksempel informasjon om utvelgelseskriterier i systemer for regelbasert automatisk analyse og vekting og hvitelister i mønstergjenkjenningssystemet[57]. I tillegg må det sørge for et manuelt apparat rundt oppfølgingen som kan sørge for at kravene til begrunnelse og klageadgang blir oppfylt.

[55] Schartum, Bygrave (2004) s 156
[56] Schartums kommentarer til personopplysningsloven note 102 til § 25, Gyldendal Rettsdata
[57] Se punkt 6.2.1 om utlevering av hvitelister m.v.

6.2 Saksbehandling

6.2.1 Generelle hensyn

Generelt er kan man stille visse krav til saksbehandlingen[58] rundt loggoppfølging, som for eksempel at den oppfyller krav i lovverk, arbeidsavtaler, tariffavtaler og bedriftens personalreglement, og at den ivaretar krav til forsvarlig saksbehandling og de ansattes rettigheter.

Utgangspunktet for ethvert kontrolltiltak rettet mot en ansatt må være at det er saklig begrunnet i virksomhetens forhold. Dette innebærer at logganalyse og oppfølging av analysen må være besluttet i virksomhetens ledelse, og en representant for ledelsen må ha fått tildelt myndighet til å gjennomføre oppfølging av logganalyse eller denne myndigheten må være delegert i organisasjonen. For at konsekvensene av et uberettiget oppslag skal være forutsigbare for den ansatte, bør rutinen rundt oppfølging av logger være dokumentert og tilgjengelig for de ansatte. Dette følger også av dokumentasjonskravene i helseregisterloven §§ 16 og 17. Nøyaktig hvilken dokumentasjon som skal være tilgjengelig for de ansatte vil avhenge av en avveining mellom fordelene ved å ha åpenhet om kontrolltiltaket og fordelene ved å holde enkelte aspekter av loggkontrollen hemmelig. Hvis sykehuset velger å gjøre for eksempel hvitelister og retningslinjer for vekting og risikoscore tilgjengelig for de ansatte, kan det føre til at de ansatte får et mer positivt forhold til kontrollen. På den andre siden risikerer man at enkelte ansatte justerer sin oppførsel for å unngå å bli fanget opp av kontrollen, og at kontrollens effektivitet dermed blir redusert. Sykehuset må vurdere hvor stor muligheten er for at offentliggjøring av detaljer rundt for eksempel hvitelister og risikoscore får konsekvenser for sikkerheten. Uansett hva sykehuset kommer fram til, må opplysningene en ansatt får være så detaljerte at han eller hun har mulighet til å gi tilsvar.

Rutinen for oppfølging av logger må sikre lik behandling av like tilfeller. Det vil si at dersom sykehuset først har bestemt at resultatene fra logganalysen skal følges opp, må alle oppslag i rapporten følges opp, eller i det minste alle oppslag av samme type. Å velge ut enkelte oppslag å følge opp, mens andre ikke blir fulgt opp, vil lett få preg av vilkårlighet.

---

[58] Det følger av rettspraksis at arbeidsgivers styringsrett begrenses av et saklighetskrav. Se for eksempel Rt. 2001 s. 418.

Man kan også argumentere for at rutinene bør sørge for at oppfølgingen av logger bør foretas av mest mulig uhildede parter. På den ene siden vil det være naturlig at ansvaret for oppfølging av ansatte ligger hos den ansattes leder, men på den andre siden kan det være fornuftig å at oppfølgingen ligger hos en uavhengig avdeling, for å unngå at det utvikler seg egne forståelser rundt omkring i avdelingene om hva som er "greie" oppslag.

Kravene til forsvarlig saksbehandling innebærer at sykehuset må sørge for at den ansatte får mulighet til å uttale seg i sakens anledning. Den ansatte må få informasjon i løpet av prosessen, og bør ha mulighet til å la seg representere av fagforeningen eller ha en tillitsvalgt med seg på møter og lignende. I tillegg må den ansatte gis adgang til å klage en eventuell avgjørelse.[59]

Personopplysningsforskriften § 2-6 er sykehuset pålegger sykehuset å ha et avvikssystem for å behandle avvik fra fastlagte rutiner for bruk av informasjonssystemet. Formålet med avviksbehandlingen er å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse. Oppfølging av logger bør inngå som en del av dette avvikssystemet.

6.2.2 Personprofiler

Ved mønstergjenkjenning blir det utarbeidet personprofiler om de ansatte. En personprofil er et uttrykk som brukes i personopplysningsloven om informasjonsmønstre som kan brukes til å gjøre antakelser om for eksempel den registrertes adferd. Hvis bruk av mønstergjenkjenning resulterer i en henvendelse til eller en avgjørelse rettet mot en ansatt, vil databehandlingen falle inn under bestemmelsen om bruk av personprofiler i personopplysningsloven § 21. Bestemmelsen sier at den registrerte har rett til informasjon om hvem som er databehandlingsansvarlig, hvilke opplysningstyper som er anvendt og hvor opplysningene er hentet fra.

Det er usikkert hvilken vekt denne bestemmelsen vil ha ved siden av ansattes rett til informasjon etter arbeidsmiljøloven § 9-2 annet punkt og personopplysningsloven § 20. Sykehuset må sørge for at alle ansatte som gjør oppslag i den elektroniske journalen, og dermed blir utsatt for kontrolltiltak, får informasjon som spesifisert i disse to

[59] Se for eksempel arbeidsmiljøloven § 4-2 om retten til medvirkning.

bestemmelsene. Dermed har den ansatte sannsynligvis allerede fått informasjonen han har rett til etter personopplysningsloven § 21.

6.3 Innsyn for pasienter

Et spørsmål i forbindelse med logganalyse, er om man kan la pasientene få innsyn i resultatene. Pasientene har innsyn i logg fra egen journal, jf. helseregisterloven § 13, sjette ledd. Når behandling av opplysninger om pasienter inngår i logganalysen, har pasientene i tillegg rett til innsyn i den utstrekning som følger av personopplysningsloven § 18. Ingen av disse innsynsrettene strekker seg så langt som til resultatene av analysen.

En eventuell utlevering av analyseresultater vil være en utlevering av personopplysninger om de ansatte, og sykehuset må ha hjemmel i personopplysningsloven for utleveringen. Vilkårene for en eventuell utlevering finnes i personopplysningsloven § 8. I utgangspunktet kan en utlevering bare skje dersom den registrerte har samtykket, eller det finnes lovhjemmel for utleveringen. Dersom samtykke ikke foreligger, og det ikke finnes lovhjemmel, kan alternativene i § 8 bokstaver a-f brukes. Kriteriet er at utleveringen må være nødvendig for å oppnå formålet som er angitt i de forskjellige alternativene. Ingen av alternativene i § 8 bokstaver a-e hjemler en utlevering til pasienter, men en mulig hjemmel vil være § 8 bokstav f som sier at behandling av opplysninger kan skje hvis det er nødvendig for at ”den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen”. Analyseresultatene kan med andre ord utleveres til pasienten hvis det er nødvendig for at pasienten skal kunne ivareta sin interesse, som i dette tilfelle vil være å beskytte sitt personvern, og hvis hensynet til den ansattes personvern ikke overstiger denne interessen.

Det er tvilsomt om utlevering av analyseresultater er *nødvendig* for at pasienten skal kunne ivareta sitt personvern, tatt i betraktning av at pasienten allerede har rett til å få loggen utlevert, og at analyseresultatene avhengig av metode kan være så usikre at nytteverdien er helt begrenset.

Utfallet av avveiningen mellom pasientenes og de ansattes personvern er ikke gitt på forhånd, men det kan argumenteres for at de ansattes personvern skal gå foran så lenge oppfølgingen av analyseresultatene ikke er gjennomført.

7 Sykehusenes plikt til å følge opp logger

7.1 Hva må logges?

Det er autorisert bruk og forsøk på uautorisert bruk som skal logges. Autorisert bruk vil i denne sammenhengen bety bruk som er autorisert etter reglene i helseregisterloven § 13 første ledd. Ettersom helsepersonellet blir ansett for å være autorisert for bruk av journalsystemet i det de får utdelt brukernavn og passord, vil det si at alle oppslag helsepersonell gjør i journalsystemet vil være autoriserte, uavhengig av om helsepersonellet har hjemmel for oppslaget eller ei.
Uautorisert bruk vil si bruk som ikke er autorisert etter helseregisterloven § 13. Det innebærer at alle mislykkede autentiseringer skal registreres. Dette registreres ikke i samme loggen som oppslag som gjøres etter vellykkede autentiseringer, og logger over mislykkede autentiseringer vil ikke bli videre behandlet her.
Det er ”bruk” av journalsystemet som skal logges. Et journalsystem brukes til daglig av ansatte ved sykehuset for å følge opp pasienter. Å lese journalnotater, dokumentere behandling, medikamentbruk og tilstand, skanne inn dokumenter, skrive ut epikriser, rette og slette journaldokumenter og skrive ut tilgangslogger er bare noen av oppgavene som utføres. En naturlig forståelse av ordet ”bruk” tilsier at alt dette skal registreres.

For at loggene skal være til nytte i avviksbehandlingen, og skal kunne brukes til å oppklare sikkerhetsbrudd, må det settes opp minimumskrav til hva loggene skal inneholde. Reglene i personopplysningsforskriften sier ikke noe detaljert om dette, men ut i fra formålet med loggføring av tilgang til journal kan man trekke konklusjoner om hva som må logges. I utgangspunktet vil informasjon om *hvem* som var pålogget, *hvilken handling* som ble utført, *tidspunkt* for oppslaget og *hvilken pasientjournal* handlingen ble utført i være minimumskrav. Denne informasjonen er nødvendig, men ikke tilstrekkelig, for å bevise at det har blitt foretatt et uberettiget oppslag.
For å avgjøre hvilken informasjon som må logges for å oppfylle formålet med loggene kan man se til aksepterte standarder for informasjonssikkerhet. Norm for

informasjonssikkerhet i helsesektoren stiller krav om at loggen i tillegg til de fire punktene over skal inneholde *rollen*, *virksomhetstilhørigheten* og *organisasjonstilhørigheten* til den som gjorde oppslaget, informasjon om *hva slags type informasjon* det er gitt tilgang til, *grunnlaget* for tilgangen, *varighet* av tilgangen og *begrunnelse* for nødrettsoppslag. Det er uklart hva forfatterne mener med uttrykket "nødrettsoppslag", men bruk av ordet nødrett tyder på at de sikter til oppslag som kan være straffrie etter straffeloven § 47, og ikke bruk av aktualiseringstilgangen generelt. NS-ISO/IEC 27002:2005 retter seg ikke mot journalsystemer spesielt, men inneholder anbefalinger om logginnhold generelt. Anbefalingene etter denne standarden omfatter den samme informasjonen som nevnt ovenfor.

Avhengig av hvilken strategi for logganalyse sykehuset velger kan det være nødvendig å ha med mer informasjon enn minimumskravene allerede nevnt. For mønstergjenkjenning vil man være avhengig av å ha informasjon om hvilken *avdeling* pasienten var innlagt på og *stillingstittelen* til den ansatte. Dette kan også være aktuelt for regelbasert automatisk analyse. For begge de automatiserte analysestrategiene kan pasientens og den ansattes *fødselsnummer* være nyttig for å få informasjon om oppslag på ansatte som også har vært pasienter og oppslag på egen journal. Behovet for informasjon må vurderes med utgangspunkt i valgt analysestrategi og sykehusets behov for et effektivt logganalysesystem som bidrar til målsetningen om tilfredsstillende informasjonssikkerhet. Forholdet til minimalitetsprinsippet og personopplysningsloven § 11 må også vurderes.

7.2 Er sykehusene forpliktet til aktivt og systematisk å følge opp logger?

For å kunne si noe om i hvilken grad det er lovpålagt å følge opp logger, må man først ta hensyn til hva som er formålet med bestemmelsene om logging.

I utgangspunktet skal loggen bidra til at sykehuset kan oppnå tilfredsstillende informasjonssikkerhet. Datatilsynet skriver i sine kommentarer til sikkerhetsbestemmelsene i personopplysningsforskriften at sykehuset skal registrere bruk av informasjonssystemet "i den grad det er nødvendig for gjennomføring av avviksbehandling, herunder oppklaring av sikkerhetsbrudd".[60] Det vil si at loggene skal eksistere som dokumentasjon på hva som har blitt gjort i informasjonssystemet. Dersom

[60] Datatilsynets kommentarer til sikkerhetsbestemmelsene i personopplysningsforskriften s. 10

man har en avvikssituasjon eller et sikkerhetsbrudd, skal man kunne bruke loggene til å kartlegge hva som skjedde. Det ligger også i sakens natur at det vil være aktuelt å bruke logger som bevis, for eksempel hvis sykehuset mistenker at en ansatt har forbrutt seg mot sikkerhetsrutiner eller lovverk.

I forbindelse med tilføying av nytt siste ledd i helseregisterloven § 13 (om pasientens rett til innsyn i tilgangsloggen fra sin journal) uttaler flertallet i Helse- og omsorgskomitéen på Stortinget at "logging av informasjon om hvem som har hatt tilgang til taushetsbelagte opplysninger, er et viktig element for å bedre informasjonssikkerheten" og at pasienters mulighet for innsyn i logg vil "bidra til å øke pasientens kontroll med opplysningene og gjøre personvernet mer betryggende".[61] Loggene skal altså også være et verktøy for pasienten, slik at han eller hun kan forsikre seg om at ingen har hatt uberettiget tilgang til journalen.

Bestemmelsene sier ikke noe direkte om loggene skal brukes proaktivt for å avdekke avvik og sikkerhetsbrudd, eller om de bare skal brukes til å oppklare avvik og sikkerhetsbrudd i tilfeller hvor sykehuset har grunn mistanke. Datatilsynets kommentarer til § 2-8 synes å forutsette at loggene først og fremst skal brukes til å etterforske og oppklare en hendelse i etterkant, og ikke skal brukes proaktivt til å oppdage avvik. Men det er vanskelig å finne noe i bestemmelsen eller kommentarene som hindrer en slik bruk.

Uttalelsene til Helse- og omsorgskomitéen i forbindelse med endringen av helseregisterloven § 13, tyder på at tanken er at loggene ikke bare skal brukes til oppklaring dersom man har en mistanke, men at pasienten skal kunne bruke loggene til å kontrollere tilgangene for å forsikre seg om at ingen har hatt uberettiget tilgang til journalen. Dette er som sagt en oppgave den behandlingsansvarlige ikke kan skyve over på pasienten, så pasientens kontroll av logger vil eventuelt komme i tillegg til den databehandlingsansvarliges kontroll av loggene.

Spørsmålet blir altså om den databehandlingsansvarlige på noen måte er forpliktet til å aktivt følge opp loggene utover å bruke dem til kontroll og bevis etter at man har oppdaget at det har vært en hendelse. Dette vil først og fremst være et spørsmål om man

[61] Innst. O. nr. 110 (2008-2009) s. 7

har andre sikkerhetstiltak på plass som sørger for at urettmessig tilegnelse av pasientopplysninger ikke kan skje, og som gjør loggoppfølging unødvendig.
I forarbeidene til endringen av helseregisterloven i 2008 (ny § 13a) skriver Helse- og omsorgsdepartementet i forbindelse med § 13 at det er et grunnleggende prinsipp av tilgang til helseopplysninger bare kan gis i den grad det er nødvendig for de ansattes arbeid, og at kravene i § 13 "innebærer at den databehandlingsansvarlige for opplysningene må organisere og tilrettelegge virksomheten på en slik måte at urettmessige tilegnelser av pasientopplysninger, herunder «*snoking*», i utgangspunktet ikke skal kunne skje". [62]
Det åpenbare sikkerhetstiltaket for å forhindre uautorisert bruk av og innsyn i journalsystemet, er tilgangskontroll. Spørsmålet er om tilgangskontroll alene eller sammen med ikke-tekniske tiltak er et tilstrekkelig sikkerhetstiltak for å beskytte informasjonen som ligger i journalsystemet , eller om det trengs ytterligere sikkerhetstiltak i form av loggoppfølging.
Da helseregisterloven ble vedtatt skrev Helse- omsorgsdepartementet at helseregisterloven § 13 "begrenser tilgangene mer enn fysiske og tekniske tilgangssperrer alene", og det forutsettes at virksomheten følger opp § 13 med tiltak som "informasjon og oppbygging av kompetanse og holdninger, eventuelt også tiltak av organisatorisk art"[63]. Departementet nevner "tilgangskontroller ved bruk av passord eller lignende" som eksempel på en teknisk tilgangssperre.[64] Det er altså på det rene at begrensningene i § 13 er større enn det man kan få til ved tilgangskontroll. Men det er uklart om departementet ikke har vurdert logger som et teknisk tiltak i det hele tatt, eller om de har ment at logger ikke er egnet som tiltak.
I sine merknader til personopplysningsforskriften § 2-14 skriver Datatilsynet at "Sikring av konfidensialitet, tilgjengelighet eller integritet kan ikke utelukkende baseres på rutiner den enkelte medarbeider forutsettes å følge. Den behandlingsansvarlige må også etablere tiltak som fungerer uavhengig av medarbeidernes handlinger".[65] Denne bestemmelsen pålegger den databehandlingsansvarlige å innføre sikkerhetstiltak som skal forhindre uautorisert bruk av informasjonssystemet. Selv om helsepersonells

[62] Ot.prp. nr. 25 (2007-2008) s. 61
[63] Ot.prp. nr. 5 (1999-2000) s. 270
[64] Ot.prp. nr. 5 (1999-2000) s. 172
[65] Datatilsynets kommentarer til personopplysningsforskriften s. 14

uberettigede oppslag i pasientjournal ikke er uautorisert bruk i den forstand, er poenget allikevel fornuftig i forhold til journalsystemer. Der hvor helsepersonellet har vid tilgang til å gjøre oppslag i journalsystemet, er det ofte bare organisatoriske tiltak som skal forhindre uberettigede oppslag. I mange tilfeller er det ikke implementert tekniske sikkerhetstiltak som ikke kan omgåes av de ansatte. Formålet med bestemmelsen er å sikre konfidensialitet, integritet og tilgjengelighet for opplysningene i informasjonssystemet, og det er vanskelig å finne en grunn til at prinsippet om at sikkerhetstiltakene skal fungere uavhengig av de ansattes handlinger ikke skal gjelde for sikkerhetstiltak i forbindelse med journalsystemet selv om alle oppslagene i utgangspunktet er autoriserte.

Året etter at § 13a ble innført, ble helseregisterloven endret for å tillate tilgang på tvers mellom sykehus. I forarbeidene til den endringen skriver Helse- og omsorgsdepartementet i forbindelse med krav til sikringstiltak mot uautorisert endring og sletting av opplysninger at ”All lesetilgang fra eksternt helsepersonell skal logges og identifiseres. Det samme skal skrivetilgang (inkludert elektronisk signering) fra eksternt helsepersonell, fortrinnsvis ved bruk av HPR-nummer”.[66]
Helse-og omsorgsdepartementet satte også i gang et arbeid med å utforme en informasjonssikkerhetsforskrift i forbindelse med sykehusenes nye mulighet til å gi tilgang til sitt journalsystem for eksterne helsearbeidere. Forskriften ble sendt ut på en andre høring i mai 2010, men er foreløpig ikke vedtatt. Forslaget til forskrift bygger videre på personvernlovgivningen i personopplysningsloven med forskrift og helseregisterloven. Forslaget inneholder bestemmelser om logging av tilgang til opplysninger i et behandlingsrettet helseregister, og hva loggene skal inneholde. Forskriften pålegger sykehusene å dokumentere hvem som har hatt tilgang til opplysninger i journalsystemet, og grunnlaget for tilgangen. [67] Denne dokumentasjonen er definert som en del av pasientens journal, og skal komme i tillegg til logger. Det skal være definert i dokumentasjonen hvilken av forslagets bestemmelser[68] som er grunnlaget for tilgangen. Formålet er å gi pasienten en kortfattet oversikt over hvem som har hatt tilgang til journalen, og hvorfor vedkommende hadde det. Departementet

[66] Ot.prp. nr. 51 (2008-2009) s. 47
[67] Forslag til forskrift om informasjonssikkerhet § 31
[68] Se forslagets §§ 19-23 for bestemmelser om tilgang

skriver at ”Ettersom dokumentasjonen vil være betydelig mer oversiktlig enn registreringen i hendelsesregistrene[69], kan det antas at den vil være et godt hjelpemiddel for pasienter som ønsker å få klarlagt om noen uberettiget har tilegnet seg opplysninger i journalen”.[70]

I tillegg til denne dokumentasjonen pålegger departementet sykehusene å føre logger over hvem som har hatt tilgang til pasientenes journaler.[71] Disse skal være mer detaljerte enn dokumentasjonen etter § 31, og skal blandt annet inneholde informasjon om nøyaktig hvilke opplysninger den ansatte hadde tilgang til.[72]

Forslaget pålegger sykehusene å jevnlig kontrollere både dokumentasjon etter § 31 og logger etter § 32. Hvis kontrollen avslører uberettiget tilgang til helseopplysninger, skal Datatilsynet og pasienten informeres.[73]

Kombinasjonen av å pålegge sykehusene å dokumentere grunnlaget for tilgangen og å pålegge dem en omfattende plikt til å kontrollere logger tyder på at departementet går ut i fra at helsepersonell ofte kan ha vide tilganger til journalsystemet, og at loggkontroll kan være et godt verktøy for å avdekke eventuell misbruk av disse tilgangene. Bestemmelsene kan også leses slik at departementet mener at organisatoriske tiltak ikke er nok for å forhindre uberettiget tilegnelse av informasjon.

Tilsynsmyndighetene har uttalt seg om vide tilganger i behandlingsrettede helseregistre og logging i en tilsynsrapport som kom etter at Datatilsynet, Statens helsetilsyn og Helsetilsynet Oslo og Akershus gjennomførte tilsyn ved Akershus universitetssykehus (Ahus) i 2006. I den ble det påpekt et avvik i forbindelse med tilgangskontroll. Tilsynsmyndighetene skriver at sykehuset ”sikrer ikke at taushetsbelagte personopplysninger i det elektroniske pasientjournalsystemet DIPS er forsvarlig vernet mot innsyn fra ansatte som ikke har legitimt behov for opplysningene”. Avviket ble begrunnet med sykehuset ga de ansatte svært vide tilganger i journalsystemet for å unngå bruk av aktualisering (kalt ”blålys” i DIPS), og i at sykehuset ikke hadde ”egnede logganalyseverktøy som gir mulighet for å avdekke uønskede hendelser, eller som gir grunnlag for å følge opp anormale hendelser. Loggjennomgang var begrenset til

[69] Hendelsesregistre er det samme som logger. Se forslagets § 32.
[70] Forslag til forskrift om informasjonssikkerhet s. 63
[71] Ibid. § 32.
[72] Ibid. s. 64
[73] Ibid. § 33.

stikkprøver på oppslag gjort på en pasient, og på kumulative rapporter om ansattes bruk av blålysfunksjonaliteten". Tilsynsmyndighetene påpekte at loggkontrollen ikke omfattet ordinære oppslag i journal, og skrev at "ansatte ved kliniske avdelinger som kikker i pasient journaler uten å ha tjenstlige behov, har med dagens ordninger lav risiko for å bli avslørt (sic)".[74]

Tilsynsmyndighetens grunnlag er pasientjournalforskriften § 4 bokstav f (som sier at journalsystemet skal være organisert slik at det er mulig å etterleve krav gitt i eller i medhold av lov), helseregisterloven §§ 13 og 16 og personopplysningsforskriften § 2-14.[75] Resonnementet synes å være at når tilgangen til journalsystemet er så vid som i dette tilfellet, kreves det et ekstra teknisk sikkerhetstiltak i form av loggjennomgang for å sikre at den vide tilgangen ikke blir misbrukt.

I tillegg oppstiller tilsynsmyndigheten et krav om at det skal være mulig å bruke et logganalyseverktøy for å "avdekke uønskede hendelser". Dette kravet er videre enn det som synes å være forventningen i kommentarene til personopplysningsforskriften, og ser ut til å ha sammenheng med de vide tilgangene i journalsystemet. Datatilsynet kan overprøve sykehusenes vurderinger når det gjelder informasjonssikkerhet med hjemmel i helseregisterloven §§ 31, jf. personopplysningsloven § 42 tredje ledd nr. 3, og 32. § 31 sier at Datatilsynet "fører tilsyn med at bestemmelsene i loven blir fulgt og at feil eller mangler blir rettet". § 32 gir Datatilsynet hjemmel til å "stille vilkår som må oppfylles for at behandlingen av helseopplysningene skal være i samsvar med loven". Datatilsynet kan ikke gi pålegg som fører til strengere regulering enn det loven krever. Vilkårene skal bringe behandlingen av helseopplysningene innenfor lovens ramme.[76] Hvor spesifikke vilkår Datatilsynet har anledning til å stille er ikke beskrevet i detalj, og det kan være gode grunner til dette. Antagelig vil det variere hvor spesifikke krav det er nødvendig å stille fra sak til sak, avhengig av kunnskapsnivå og interesse hos virksomheten. Vilkårene Datatilsynet stiller må rette seg mot en behandling av helseopplysninger som er i strid med loven eller bestemmelser i medhold av loven[77]. Det vil si at Datatilsynet må gjøre en konkret vurdering i hvert tilfelle. I og med at vilkårene gjelder en spesifikk behandling av personopplysninger, må også vilkårene

[74] Rapport fra tilsyn med konfidensialiteten og tilgjengeligheten til elektronisk pasientjournal ved Akershus universitessykehus HF s. 5-6.
[75] Ibid.
[76] Ot.prp. nr 5 (1999-2000) s. 293
[77] Helseregisterloven § 32 første ledd

kunne være ganske spesifikke. Datatilsynet har sannsynligvis anledning til å stille vilkår om loggkontroll på bakgrunn av de vide tilgangene ved Ahus. Om de har anledning til å stille vilkår om hvordan loggkontrollen skal gjøres er mindre sikkert, men ut i fra beskrivelsen av de dårlige mulighetene for manuell kontroll av logger i tilsynsrapporten[78], er det antagelig grunnlag for at Datatilsynet kan gjøre det i dette tilfellet. Om Datatilsynet kan gå så langt som til å sette som vilkår at en behandlingsansvarlig må bruke en spesiell strategi for logganalyse vil komme an på omstendighetene i det konkrete tilfellet hvor det kan bli aktuelt. Hvis logganalysesystemer får innpass i helsesektoren, og man får erfaring nok med teknologien til å si at en strategi er bedre enn en annen, vil det være mulighet også å stille krav om dette.
Tilsynsrapporten viser at Datatilsynet ser en sammenheng mellom for vide tilganger og behov for loggkontroll, og at ved sykehus hvor de ansatte har vide tilganger i journalsystemet kan loggkontroll være nødvendig for å oppnå tilfredsstillende informasjonssikkerhet.

Spørsmålet om systematisk oppfølging av logger er også behandlet i flere standarder for informasjonssikkerhet. Disse standardene er ikke bindende, men sier noe om hva fagmiljøene mener er god informasjonssikkerhet. Standardene kan fungere som veiledere for sykehusene i arbeidet med å fastlegge akseptabel risiko, gjøre risikovurderinger og bestemme hvilke tiltak som skal innføres.
I følge Norm for informasjonssikkerhet i helsesektoren skal rutinene for tildeling av autorisasjon sikre at bare ”teknisk personell med særskilt behov for tilgang” har tilgang til ”større mengder” helse- og personopplysninger[79].
Normens regler om kontrolltiltak sier at all autorisert og forsøk på uautorisert bruk av systemene skal registreres, og at hendelsesregistrene ”enkelt” skal kunne analyseres ved hjelp av analyseverktøy for å oppdage uberettiget tilegnelse av informasjon.[80] I tillegg stiller den krav om at all bruk av nødrettstilgang skal dokumenteres, og at hvert enkelt tilfelle skal følges opp som et avvik for å sjekke at tilgangen var berettiget. Normen sier

[78] Rapport fra tilsyn med konfidensialiteten og tilgjengeligheten til elektronisk pasientjournal ved Akershus universitessykehus HF
[79] Norm for informasjonssikkerhet i helsesektoren s. 22
[80] Norm for informasjonssikkerhet i helsesektoren s. 23

at det skal etableres prosedyrer for å sørge for at loggene blir analysert fortrinnsvis hver uke, slik at hendelser kan oppdages før de får alvorlige konsekvenser.[81]
Den internasjonale standarden NS-ISO/IEC 27002:2005 inneholder også anbefalinger om logging. Den sier at på grunnlag av en risikovurdering bør databehandlingsansvarlig innføre logging av bruk av informasjonsbehandlingssystemer. Resultatene fra loggingen bør gjennomgås jevnlig.[82] Hvor ofte gjennomgangen skal skje bør avhenge av en risikovurdering som tar hensyn til blant annet hvor kritisk systemet er, hvor sensitiv informasjonen som er lagret der er og tidligere erfaringer med uberettiget bruk.[83]

Spørsmålet om logging av tilgang til helseopplysninger har ikke vært behandlet direkte i domstolene, men Den europeiske menneskerettighetsdomstolen hørte i 2008 saken I v. Finland. Saken omhandler en sykepleier som jobbet på et sykehus hvor hun også var pasient. Hun fikk etterhvert inntrykk av at hennes kolleger hadde vært inne og lest journalen hennes. Etter å ha tapt to rettssaker i Finland, klaget hun Finland inn for Den europeiske menneskerettighetsdomstolen for brudd på Den europeiske menneskerettighetskonvensjonens artikkel 8. Klagen var basert på at finske helsemyndigheter ikke hadde oppfylt sin forpliktelse etter finsk lov til å beskytte hennes helseopplysninger mot innsyn. Hennes pasientjournal var tilgjengelig for alle ansatte på sykehuset, og journalsystemet logget bare de 5 siste oppslagene. I tillegg inneholdt loggene ikke navn på helsepersonellet, men bare seksjonen de jobbet på. Loggen ble også slettet når journalen ble returnert til arkivet. Länsstyrelsen i Finland skrev i et svar på en klage fra saksøker i forkant av rettssakene i Finland at ”the system should record any consultation of patient files as a safeguard for privacy in order to ensure that the responsibility for a possible leak of information can be individualized”.
Den europeiske menneskerettighetsdomstolen fant at Finland ikke hadde oppfylt sin positive forpliktelse til å sørge for at saksøkerens rett til privatliv ble ivaretatt. Domstolen baserer avgjørelsen på at Finland på utleveringstidspunktet hadde lovgivning som forpliktet sykehuset til å sørge for at pasientenes journaler var beskyttet mot uautorisert innsyn, og at det bare skulle være personell involvert i behandlingen av pasienten som hadde tilgang til en pasients journal. Disse forpliktelsene ble ikke

[81] Ibid.
[82] NS-ISO/IEC 27002:2005 s. 56
[83] NS-ISO/IEC 27002:2005 s. 57

oppfylt. I tillegg vant saksøker ikke fram i retten i Finland fordi det ikke var mulig å bevise at noen hadde hatt uautorisert tilgang til hennes pasientjournal på grunn av den dårlige loggmekanismen. Menneskerettighetsdomstolen fant at Finland, ved å plassere bevisbyrden for at det skulle ha skjedd et ulovlig oppslag på saksøkeren, overså det faktum at sykehuset ikke hadde sørget for tilfredsstillende sikring mot uautorisert tilgang til pasientjournaler. Menneskerettighetsdomstolen skriver at "It is plain that had the hospital provided greater control over access to health records by restricting access to health professionals directly involved in the applicant's treatment or by maintaining a log of all persons who had accessed the applicant's medical file, the applicant would have been placed in a less disadvantaged position before the domestic courts".[84] Domstolen kommenterte også at dersom forpliktelsene etter finsk lov hadde blitt oppfylt, ville det ha vært "a substansial safeguard" for saksøkerens rettigheter etter menneskerettighetskonvensjonens artikkel 8.
Menneskerettighetsdomstolen synes her å se det samme forholdet mellom vide tilganger og logging som Datatilsynet. Resonnementet ser ut til å gå ut på at hvis tilgangene skal være vide må man kunne få en oversikt over hvem som har vært inne og lest journalen. Dommen kan ikke tas til inntekt for en forpliktelse for sykehusene til å aktivt og systematisk følge opp logger. Avgjørende for domstolen var at journalsystemet ved sykehuset ikke var organisert på den måten som ble pålagt i finsk lovgivning.[85] Dommen kan tolkes slik at den pålegger stater en positiv forpliktelse til å sørge for at lovgivning som skal beskytte borgernes rett til privatliv blir fulgt, og til å sørge for at det blir implementert tiltak som oppfyller formålet med lovgivningen. Det holder altså ikke bare å ha bestemmelser som sier noe om hvor god informasjonssikkerheten skal være, det er også nødvendig med konkrete tiltak. For Norges del kan det bety at man har en forpliktelse til å følge opp logger hvis risikovurderinger viser at helsepersonell har så vide tilganger til journalsystemet at de uberettiget kan tilegne seg informasjon fra journaler.

Argumentasjonen rundt logging i forarbeider og tilsyn synes å lede til at sykehusene kan være forpliktet til å systematisk følge opp logger for å oppnå tilfredsstillende informasjonssikkerhet. Logganalyse vil være aktuelt som sikkerhetstiltak der hvor

[84] I v. Finland avsnitt 44
[85] Ibid.

tilgangene til journalsystemet er organisert slik at de ansatte har en vid tilgang til å gjøre oppslag, enten ved hjelp av vanlige oppslag eller ved hjelp av aktualisering, og tilgangskontrollen er det eneste sikkerhetstiltaket bortsett fra organisatoriske tiltak som beskytter pasientjournaler mot uautorisert innsyn. Det synes også å være en forutsetning av logganalysen skal være mer effektiv enn den manuelle kontrollen er i dag, særlig gjelder dette i argumentasjonen til tilsynsmyndigheten.

Selv om kravene til logging i Norm for informasjonssikkerhet i helsesektoren ikke er bindende, er kravene et uttrykk for hva som kan anses som tilfredsstillende informasjonssikkerhet i forbindelse med tilgang til helseopplysninger i journalsystemet. Det samme gjelder NS-ISO/IEC 27002:2005 som selv om den ikke retter seg spesifikt mot systemer som behandler helseopplysninger, er en anbefaling fra et internasjonalt fagmiljø.

Dommen fra Den europeiske menneskerettighetsdomstolen tyder på at det kan eksistere en forpliktelse til å følge opp logger hvis det er nødvendig for å forhindre og avsløre uberettiget tilegnelse av informasjon.

Samlet sett synes det å være gode argumenter for at sykehusene i en viss grad kan være forpliktet til å aktivt og systematisk følge opp logger. Forpliktelsen vil avhenge av hvordan tilgangskontrollen til journalsystemet er organisert og hvilke andre sikkerhetstiltak som finnes for å forhindre uberettiget tilegnelse av informasjon. Det synes å være klart at tilgangskontroll slik den ofte er organisert i sykehusene i dag, med enten vid aktualiseringstilgang eller vide ordinære tilganger, ikke alene er nok til å oppfylle kravet om tilfredsstillende informasjonssikkerhet. Organisatoriske tiltak i tillegg oppfyller ikke kravet om at de ansatte ikke skal kunne omgå tiltakene. Dermed står man igjen med systematisk oppfølging av logger som et realiserbart alternativ som kan bidra til at informasjonssikkerheten blir tilfredsstillende.

7.3 Hvilken analysestrategi egner seg best?

Hvilken strategi for logganalyse som egner seg best vil avhenge av mengden informasjon som skal analyseres og målsetningen med analysen.

For sykehus med et stort antall oppslag vil manuell kontroll egne seg dårlig. Å manuelt kontrollere oppslag er tidkrevende og selv med et intensivt arbeid vil man bare rekke gjennom en svært liten del av oppslagene. For å få bukt med en stor mengde oppslag kan sykehuset være nødt til å velge ut tilfeldige oppslag for kontroll, for eksempel ved

stikkprøvekontroll. Det kan gjøre kontrollen enda mindre effektiv ettersom sykehuset da risikerer å bruke mye tid på å kontrollere oppslag som ikke er uberettigede, mens mange uberettigede oppslag ikke blir utsatt for kontroll. Avhengig av hvordan tilgangene er organisert, kan det samme gjelde kontroll av aktualiseringslogger.

Uttalelser fra tilsynsmyndigheten viser at de ikke er fornøyde med de manuelle kontrolltiltakene som finnes ved enkelte norske sykehus.[86] Hvis man går ut i fra at sykehusene har en forpliktelse til å følge opp logger systematisk, er manuell kontroll sannsynligvis den minst egnede strategien. Med store mengder data å analysere synes manuell kontroll å være så lite effektivt at dersom sykehuset først har bruk for å innføre sikkerhetstiltak i form av logganalyse vil denne strategien antagelig ikke være tilstrekkelig. Bruken av manuell kontroll bør begrenses til tilfeller hvor sykehuset har en begrunnet mistanke om at en ansatt har uberettiget tilegnet seg tilgang til en pasients journal.

Automatisk regelbasert analyse kan redusere faren for at oppslag blir plukket ut ved tilfeldigheter, og bidrar således til større effektivitet enn ved manuell kontroll. Men selv om oppslagene blir plukket ut på grunnlag av kriterier som skal beskrive uberettigede oppslag eller uønsket adferd, kan disse kriteriene være så svake indikatorer at det allikevel må gjøres et stort oppfølgingsarbeid i etterkant av analysene. Det avgjørende for effektiviteten til et slikt analysesystem er at sykehuset klarer å begrense antallet falske positive og negative som en følge av svake indikatorer. Derfor kan strategien fungere best for mindre sykehus som har et mindre antall oppslag, relativt avklarte arbeidsforhold og –rutiner for de ansatte og liten bruk av vide tilganger for de ansatte. Da vil det være lettere for sykehuset å definere kriterier for utvelgelse, og disse vil kunne være mer presise. Det vil redusere faren for falske positive og negative, og vil øke et logganalysesystems effektivitet sammenlignet med manuell kontroll. Hvis sykehuset i tillegg har kildedata av høy kvalitet og gode rutiner for på- og avlogging av brukere, kan resultatene av regelbasert automatisk analyse gi sykehuset et godt utgangspunkt for å sjekke oppslag som kan være uberettigede.

For store sykehus med svært store oppslagsmengder, vide tilganger til journaler og

---

[86] Rapport fra tilsyn med konfidensialiteten og tilgjengeligheten til elektronisk pasientjournal ved Akershus universitetssykehus HF.
Rapport frå tilsyn med informasjonstryggleiken ved pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS ved Helse Bergen HF, Haukeland universitetssjukehus

arbeidsforhold og samarbeid mellom avdelinger som vanskelig lar seg beskrive som maskinlesbare regler utpeker mønstergjenkjenning seg som det beste alternativet. Ved å analysere tilgangslogger for å finne hva som er normal bruk av journal eliminerer mønstergjenkjenning behovet for å beskrive hva som kjennetegner et uberettiget oppslag, og dermed faren for falske positive og negative som oppstår som følge av dette. Strategien tar hensyn til interaksjoner mellom pasienter og ansatte på forskjellige avdelinger og forskjellige oppslagsmønstre avhengig av de ansattes arbeidsoppgaver og avdelingstilhørighet. Med riktig justering av parametrene og vektingen som brukes i systemet, kan sykehuset få et godt bilde av det normale oppslagsmønsteret til avdelinger og enkeltpersoner, og med det øke sjansene for at de oppslagene som blir plukket ut fordi de er unormale faktisk er uberettigede oppslag, og redusere behovet for manuell oppfølging av analyseresultatene. For å få best mulig resultater er også mønstergjenkjenning avhengig av at de ansatte følger gode rutiner for på- og avlogging, og at de ikke deler passord seg i mellom.
Mønstergjenkjenning gir også mulighet for å rangere oppslag slik at loggkontrolløren kan konsentrere seg om de mest alvorlige bruddene på taushetsplikten først. Store sykehus er avhengige av denne typen effektivitet for å kunne gjennomføre logganalyse og få gode resultater som bidrar til tilfredsstillende informasjonssikkerhet.

8 Konklusjon

Kravet om tilfredsstillende informasjonssikkerhet i helseregisterloven § 16 innebærer at sykehusene kan være forpliktet til å følge opp logger på en aktiv og systematisk måte for å avsløre uberettigede tilganger. Det vil avhenge av hvordan tilgangen til journalsystemet er organisert og hvilke andre sikkerhetstiltak som finnes for å forhindre uberettigede oppslag. Slik mulighetene er for tilgangsstyring i mange journalsystemer i dag, er tilgangskontroll ikke et godt nok sikkerhetstiltak alene ved sykehus med behov for oppslag på tvers av avdelinger. Logganalyse er i tråd med anbefalinger fra internasjonale fagmiljøer innenfor informasjonssikkerhet og signalene fra lovgivere, Sosial- og omsorgsdepartementet og Datatilsynet tyder på at krav om logganalyse kan være på vei inn i norsk lovgivning.

For at logganalyse skal være et effektivt sikkerhetstiltak må det stilles visse krav til effektivitet og etterettelighet. Manuell kontroll vil egne seg dårligst i så måte, mens regelbasert automatisk analyse egner seg best for mindre sykehus med tydelige tilgangsbegrensninger. Mønstergjenkjenning vil være den best egnede metoden for store sykehus med stor variasjon i behovet for tilgang hos de ansatte.

9 Litteraturliste

Andresen, H., O.G. Aasland Helsepersonells håndtering av pasientopplysninger Tidsskrift for Den Norske Legeforening 2008:24. http://www.tidsskriftet.no/index.php?seks_id=1781321 (hentet 18.04.2011)

Bygrave, Lee A. Data Protection Law. Approaching Its Rationale, Logic and Limits. Den Haag, Nederland. 2002.

Fosse, Gro Anita [et.al]. Er vi egentlig så sikre? Prosjektoppgave ved masterstudiet i helse- og sosialinformatikk innlevert ved Universitetet i Agder, 2010

Datatilsynets kommentarer til sikkerhetsbestemmelsene i personopplysningsforskriften. http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/SV100_00.pdf (hentet 18.04.2011)

Datatilsynet. *Sviktende tilgang i elektroniske pasientjournaler? Lovforslag om å tillate direkte tilgang til pasientjournaler på tvers av virksomhetsgrensene.* Rapport april 2009. http://www.datatilsynet.no/upload/Ttilgang%20p%C3%A5%20tvers_270409.pdf (hentet 18.04.2011)

Krogstad, Inge Mønstergjenkjenning for å avsløre misbruk av tekniske tilganger. Sluttrapport fra pilot ved Oslo universitetssykehus – Ullevål. SAS Institute, Oslo, august 2009

Krogstad, Inge [et.al]. *Sluttrapport Fagruppen Mønstergjenkjenning Fase 1* SAS Institute, Oslo, oktober 2010.

Norm for informasjonssikkerhet i helse-, omsorgs, og sosialsektoren. 2. juni 2010. http://www.helsedirektoratet.no/vp/multimedia/archive/00296/Norm_for_informasjo_296439a.pdf (hentet 24.04.11)

Norsk Standard NS-ISO/IEC 27002:2005 Informasjonsteknologi. Sikkerhetsteknikk. Administrasjon av informasjonssikkerhet. Standard Norge 2009.

Rapport fra tilsyn med konfidensialiteten og tilgjengeligheten til elektronisk pasientjournal ved Akershus universitetssykehus HF. Helsetilsynet i Oslo og Akershus, Statens Helsetilsyn, Datatilsynet. 03.01.2007. http://www.helsetilsynet.no/no/Tilsyn/Tilsynsrapporter/Akershus/2006/Elektronisk-pasientjournal-Akershus-universitetssykehus-HF-2006/ (hentet 18.04.2011)

Rapport frå tilsyn med informasjonstryggleiken ved pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS ved Helse Bergen HF, Haukeland universitetssjukehus. Helsetilsynet i Hordaland, Statens Helsetilsyn, Datatilsynet.

06.09.2006.
http://www.helsetilsynet.no/no/Tilsyn/Tilsynsrapporter/Hordaland/2006/Pasientadministrative-systemet-PIMS-Helse-Bergen-HF-Haukeland-2006/ (hentet 18.04.2011)

Rikshospitalet. *Gjennomgang og oppfølging av aktualiseringslogg i DocuLive og Klinisk Portal.* Intern rutine 1.EPJ.7.01 versjon 3.02

Schartum, Dag Wiese *Kommentarer til personopplysningsloven, note 102 til § 25*, Gyldendal Rettsdata

Schartum, Dag Wiese *Krav til sikring av personopplysninger*. I: Jansen, Arild og Dag Wiese Schartum Informasjonssikkerhet – Rettslige krav til sikker bruk av IKT. Bergen, 2005. s. 98-137.

Schartum, Dag Wiese og Lee A. Bygrave *Personvern i informasjonssamfunnet – En innføring i vern av personopplysninger*. Bergen, 2004.

9.1 Lov- og forarbeidsregister

1967	Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) av 10. februar 1967
1997	Lov om folketrygd (folketrygdloven) av 28. februar 1997 nr. 19
1999	Lov om pasientrettigheter (pasientrettighetsloven) av 2. juli 1999 nr. 63
1999	Lov om helsepersonell m.v. (helsepersonelloven) av 2. juli 1999 nr. 64
2000	Lov om behandling av personopplysninger (personopplysningsloven) av 14. april 2000 nr. 31
2001	Lov om helseregistre og behandling av helseopplysinger (helseregisterloven) av 18. mai 2004 nr. 24
2005	Lov om arbeidsmiljø, arbeidstid og stillingsvern m.v. (arbeidsmiljøloven) av 17. juni 2005 nr. 62
2000	Forskrift om behandling av personopplysninger (personopplysningsforskriften) av 15. desember 2000 nr 1265
2001	Forskrift om pasientjournal (pasientjournalforskriften) av 21. desember 2001 nr 1385

Ot.prp. nr. 92 (1998-99)	Om lov om behandling av personopplysninger (personopplysningsloven)

Ot.prp. nr. 5 (1999-2000)	Om lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
Ot.prp. nr. 25 (2007-2008)	Om lov om endringer i helsepersonelloven og helseregisterloven (krav til helsepersonells attester, erklæringer o.l., administrative reaksjoner og forbud mot urettmessig tilegnelse av helseopplysninger)
Ot.prp. nr. 51 (2008-2009)	Om lov om endringer i helseregisterloven og helsepersonelloven (tilgang til behandlingsrettede helseregistre på tvers av virksomhetsgrenser og etablering av behandlingsrettede helseregistre på tvers av virksomheter)
Innst. O. nr. 110 (2008-2009)	Innstilling fra helse- og omsorgskomiteen om lov om endringer i helseregisterloven og helsepersonelloven (tilgang til behandlingsrettede helseregistre på tvers av virksomhetsgrenser og etablering av behandlingsrettede helseregistre på tvers av virksomheter)

Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre

EP/Rdir 95/46/EF	Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.

9.2 Domsregister

I vs. Finland	Den europeiske menneskerettighetsdomstolen 17.07.2008 http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=20511/03&sessionid=69855654&skin=hudoc-en (hentet 18.04.2011)
Rt. 2001 s. 418 (Kårstø)	

10 Lister over tabeller og figurer m v