Ledningsnätverket för Medicinsk Teknik

Utredning

Patientdatalagen i den kliniska vardagen

- Vilka krav ställs på medicintekniska produkter?

Rapport version 3.0

2015-01-23

1 Sammanfattning

Personal som arbetar med medicinsk teknik/IT inom svensk sjukvård upplever vid återkommande tillfällen att de ställs inför konfliktsituationer som uppstår på grund av de icke harmoniserande regelverken avseende skyddet av patientens personliga integritet (Patientdatalagen) respektive patientsäkerheten ur ett tekniskt/fysiologiskt perspektiv (Lagen om medicintekniska produkter).

För att försöka bringa klarhet i den aktuella situationen, uppmärksamma leverantörer och tillverkare av medicintekniska produkter på problematiken, ge signaler till berörda myndigheter inför beredning av eventuella förändringar i regelverket, samt framför allt ge vägledning för personal verksam i den kliniska vardagen genom att åstadkomma ett försök till nationell samsyn, har en arbetsgrupp på uppdrag av LfMT arbetat med dessa frågor under år 2014.

Ledningsnätverket för Medicinsk Teknik (LfMT) är sjukvårdshuvudmännens (landstingens/ regionernas) gemensamma forum för samverkan, erfarenhetsutbyte och utveckling inom det medicintekniska området.

Mot bakgrund av vår genomlysning av den aktuella situationen, anser arbetsgruppen:

- Att information från en medicinteknisk produkt (MTP) ska finnas tillgänglig när den behövs i patientens vårdsituation.

- Att patientens integritet ska skyddas i tillräcklig omfattning, utan att förhindra eller försämra den vård som patienten är i behov av.

- Att det i dagens regelverk existerar en gråzon mellan inhämtandet av biologiska mätdata från patienten och när dessa data definitionsmässigt enligt Patientdatalagen (PDL) är att betrakta som journalhandling.

- Att ett nytt begrepp ***MT-data*** införs, vilket av arbetsgruppen definieras som:
  ”Tekniskt genererad (insamlad/bearbetad) information från medicinteknisk produkt av biologiska (d.v.s. anatomiska, fysiologiska, kemiska, mikrobiologiska etc.) mätdata och/eller avbildningar från en patient (d.v.s. personuppgifter i form av mätdata), vilka ännu ej av legitimerad vårdpersonal bedömts vara autentiska och väsentliga för patientens diagnostik eller vård och därmed föremål att journalföras i patientens ordinära journal”.

- Att MT-data som grundat på bedömning av klinisk personal har en väsentlig betydelse för den enskilda patientens fortsatta vård och behandling, i enlighet med PDL definieras som journalhandling och ska därmed sparas i den ordinära journalen, vilken lyder under PDL.

- Att när MT-data journalförs i patientens ordinära journal eller i en sekundär journal benämns den därefter som en journaluppgift/undersökningsresultat.

- Att MT-data är att betrakta som en personuppgift, och hanteringen av dessa, så länge de lagras i aktuell medicinteknisk produkt (MTP), därmed lyder under Personuppgiftslagen (PUL).

- Att vid åtkomst till MT-data i annat syfte än vidare vård och behandling av enskild patient, t.ex. i samband med servicearbete, gäller de krav som anges i PUL.

- Att när en medicinsk åtgärd påbörjas så har patienten samtidigt, underförstått, gett sitt samtycke till hanteringen av de personuppgifter som skapas, samt till den organisation och den tekniska miljö som informationen hanteras i.

- Att utformning av åtkomst till information måste vara lämplig för sin avsedda användning och att huvudansvaret för detta ligger på tillverkaren av MTP.

- Att Vårdgivaren å sin sida skall se till att det sammanhang som aktuell MTP används i är adekvat utformat, samt att metoder, rutiner och användning i enlighet med tillverkarens anvisningar sker av utbildad personal med behörighet för uppgiften.

- Att det inte är rimligt att få tillverkarna av MTP respektive medicinska informationssystem (MIS) att bygga in tekniska lösningar som är kopplade till Ineras säkerhetstjänster om autentisering, patientens medgivande och spärr av information. Sverige är en liten marknad som i huvudsak importerar den MTP som används i vården. Vår bedömning är att hanteringen av dessa tjänster måste ske i eller via MTP/MIS där tillverkarens avsedda användning är att hantera patienters journaler.

- Att uthopp från journalsystem till MTP som sker från journalsystem regleras av PDL.

- Att då MT-data överförs elektroniskt till journalsystem ska detta ske på ett sådant sätt att informationen inte kan avlyssnas av obehöriga eller förvanskas på vägen.

- Att då flera än en vårdgivare lagrar MT-data i en gemensam databas och där syftet är medicinsk uppföljning, måste informationen vara indexerad på ett sådant sätt att filtrering och åtkomst kan göras så att både PUL och PDL kan uppfyllas i tillämpliga delar.

- Att vid förändring av tillverkarens behörighetssystem avseende åtkomst till MTP, måste vårdgivarens personuppgiftsansvarige, i enlighet med Patientsäkerhetslagen (PSL), bygga vidare på MTP-tillverkarens riskanalys i syfte att förhindra att nya risker för vårdskador uppstår.

- Att tillverkaren enligt Lagen om medicintekniska produkter (LMP) bär huvudansvaret för att i sin riskanalys försäkra sig om att en ökad säkerhetsnivå för skydd av patientens integritet inte samtidigt ökar risken för vårdskador.

- Att vårdgivaren, i samråd med tillverkaren, anpassar och begränsar skyddet av de person-/patientuppgifter som vårdgivaren behandlar, utifrån den medicintekniska produktens avsedda användning och hantering av personuppgifter.

- Att det är positivt att utredningen om rätt information i vård och omsorg (SOU 2014:23) närmar sig LMP genom att ge förslag på:
- Styrning av behörigheter utifrån personuppgiftens avsedda användning.
- Ändamålsenlig utformning behörighetssystem.
- Riskanalyser av behörighetssystem vad avser risk för patientskada och kränkning av integritet.

- Att SKL i den fortsatta dialogen om slutbetänkandet från SOU 2014:23 (*"Rätt information i rätt tid för rätt användare"*) driver följande frågor**:**
- Ett förtydligande om hur förslaget till ny Hälso- och sjukvårdsdatalag förhåller sig till LMP.
- Definition och införande av ett nytt begrepp MT-data.
- Att Läkemedelsverket ges i uppdrag att ta fram en föreskrift om behörighetssystem på MTP riktat till tillverkarna av MTP.

Kort och koncis grund för våra påståenden.
Patienten har en rättighet att, när MTP används, erhålla en säker och ändamålsenligt god hälso- och sjukvård.

Riskanalys ska ligga som grund för att minimera risken för patienten att bli skadad eller erhålla en försämrad vård eller få sin integritet kränkt.

Det råder inte något motsatsförhållande mellan krav på att skydda patienten från fysisk skada och skydd av patientens integritet. Båda skydden bör tillverkaren av MTP utforma så bra som möjligt utan att de inverkar negativt på varandra.

All teknik som används i ett medicinskt syfte är att betrakta som en MTP i enlighet med LMP.

Elektroniska journalsystem, ingår i gruppen medicinska informationssystem (MIS), är MTP och lyder under lagen om medicintekniska produkter.

MT-data som genereras, insamlas, bearbetas, registreras etc. i MTP, och som inte är avsedd för att ingå i patientens journal, är ingen journaluppgift. Det är en personuppgift i enlighet med PUL och skall behandlas i enlighet med PUL.

MT-data som av legitimerad vårdpersonal bedöms som autentisk och väsentlig för patientens vård och behandling ska journalföras som undersökningsresultat i patientens ordinära journal enligt PDL.

Undersökningsresultat ska journalföras i MTP som av tillverkaren är avsedd att användas för att journalföra patientuppgifter och hantera journalhandlingar.

Det finns en övertolkning av PDL:s definition av uttrycket *"journalhandling".* En personuppgift definieras inte som en journalhandling utifrån den tekniska miljön som den hanteras i, utan av om ansvarig vårdpersonal bedömer att informationen är väsentlig för patientens vård och behandling och därmed ska journalföras.

Merparten av den MTP som används i rutinvård och som hanterar MT-data är inte av tillverkaren avsedd för att hantera patientens journal.

Den information som PDL reglerar hanteras av MTP enligt LMP. Förvirringen som råder om hur vårdverksamheterna både ska klara patientenssäkerheten och skydd av patientens integritet har sin grundorsak i att PDL och LMP inte harmoniserar med varandra. Detta kan leda till att patienten i en vårdsituation inte ges rätt vårdåtgärd med mycket allvarliga medicinska konsekvenser för patienten!

Socialdepartementet rekommenderas av LfMT att skapa ett gemensamt lagrum för både patientens personuppgifter och för medicintekniska produkter. Socialdepartementet bör ta ett initiativ i syfte att förbättra EU:s direktiv för medicintekniska produkter (MDD) så att det också regler patientens integritetsskydd i MTP/MIS.

2 Innehållsförteckning

3 Förord

Ledningsnätverket för Medicinsk Teknik (LfMT) är sjukvårdshuvudmännens gemensamma forum för samverkan, erfarenhetsutbyte och utveckling inom det medicintekniska området. I LfMT deltar sjukvårdshuvudmännens medicintekniska chefer/motsvarande (www.lfmt.se). Inom ramen för LfMT:s verksamhet finns sedan 2011 ett nationellt nätverk med personer vilka arbetar som *System Integrator* (SI) eller har motsvarande funktioner hos sin respektive arbetsgivare.

LfMT upplever idag en konflikt mellan dels gällande krav på patientsekretess enligt patientdatalagen, dels de möjligheter och begränsningar som dagens medicintekniska utrustningar och system erbjuder i samband med implementeringen av dessa krav. LfMT tillsatte därför under 2014 en arbetsgrupp bestående av medlemmar från SI-nätverket vilka gavs uppdraget att utreda det faktiska nuläget, samt analysera och föreslå riktlinjer kring hur denna konflikt kan hanteras.

Rapporten vänder sig främst till vårdgivare och berörda myndigheter, men även till leverantörer och tillverkare av medicintekniska utrustningar och system.

4 Medverkande

Uppdragsägare och mottagare av resultat:
Styrelse LfMT

Uppdragsledare:
Petter Eriksson, Örebro läns landsting

Uppdragsmedlemmar:
Jan-Olof Dahlberg, Västerbottens läns landsting
Kjell Andersson, Västra Götalandsregionen
Mikael Frick / Stig Wiinberg, Region Skåne

Personer som arbetsgruppen varit i kontakt med:
Patrik Sundström, Utredningssekreterare, Utredningen om rätt information i vård och omsorg (SOU 2014:23)
Helena Dzojic, Enhetschef Medicinsk teknik, Läkemedelsverket (LV)
Magnus Bergström, IT-säkerhetsspecialist, Datainspektionen (DI)
Övriga medlemmar i SI-nätverket
M.fl.

A. Inledning

5 Bakgrund

Patientdatalagen (PDL) kom år 2008 för att säkerställa patientens integritet samtidigt som den öppnade upp mot nya funktioner så som sammanhållen journalföring och möjlighet att ge patienten direktåtkomst till sin journal via fria medier så som internet.

Traditionellt sett har medicinteknisk utrustning oftast verkat självständigt. Sjukvårdspersonal har använt utrustningen för att diagnosticera och behandla samt i samband med detta erhållit mätvärden, grafik, bilder och analyser. Utvalda delar av denna information som har ansetts väsentliga har dokumenterats i patientens journal.

Med tiden har dessa utrustningar blivit alltmer IT-anpassade och i vissa fall vuxit samman till system, vilka nu i många fall har stöd för att både samla in och lagra medicinsk information i egna databaser. Åtkomst till den lagrade informationen ges via olika gränssnitt och behörigheten till dessa system är därmed inte direkt kopplad till utrustningens fysiska placering.

Konkret har detta inneburit att både relevant och irrelevant information som genererats från medicinteknisk utrustning sparats i samma informationsdatabas. Det råder också en stor variation av hur åtkomst från patientens journal skapas till dessa informationsdatabaser.

6 Problembeskrivning

Medicintekniska produkter (MTP) är i varierande grad och utformning försedda med skydd av patientens personuppgifter. Regelverket för MTP innehåller ringa information och vägledning om hur integritetsskydd ska utformas. Informationssäkerhetsexperter anser att alla MTP som innehåller patientuppgifter ska anpassas till PDL, vilken riktar sig till vårdgivarna. Motsvarande regelverk som riktar sig till tillverkarna av MTP saknas. Informationssäkerhetsexperterna vill att vårdgivarna via sina upphandlingar anger krav på hur integritetsskydd i MTP ska utformas. Tillverkarna har svårt att hantera dessa krav och utformningen av kraven på integritetsskydd uppfattas av vissa tillverkare som ett hinder. De hävdar att det blir svårare att använda MTP för avsedd medicinsk användning och att risken att patientsäkerheten försämras av otillgänglighet är påtaglig. Internationella tillverkare av MTP ställer sig oförstående till den lokala svenska PDL.

Den information som PDL reglerar hanteras av MTP enligt Lagen om medicintekniska produkter (LMP). Förvirringen som råder om hur vårdverksamheterna både ska klara patientenssäkerheten och skydd av patientens integritet har sin grundorsak i att PDL och LMP inte samverkar. De båda regelverken korrelerar inte med varandra!

Uppfattningen bland informationssäkerhetsansvariga att vårdgivaren, via sina kravspecifikationer, ska förmå tillverkaren att förse sina MTP med, för Sverige, unika behörighetsskydd är beteenden som kommer från traditionella IT-verksamheter. Den internationella medicintekniska industrin, som levererar merparten av MTP, har stora svårigheter att hantera dessa, för den svenska marknaden, specifika krav.

Under utredningsarbetet har vi i arbetsgruppen kunnat konstatera att det ute i vårdverksamheten finns stora svårigheter att hantera de ibland motstridiga kraven från PDL respektive LMP. Det är ett stort återkommande problem för alla inblandade parter i vårdverksamheten att veta vilket lagrum som man i första hand ska tillgodose.

7 Syfte

Projektets syfte kan i huvudsak sammanfattas i följande fem punkter:

- Att utreda hur LMP står i relation till PDL.
- Att tydliggöra krav enligt PDL på hur vårdgivaren skall hantera medicintekniska produkter och den information som dessa genererar och behandlar.
- Att öka medvetenheten och kunskapen hos medarbetare i organisationer som förvaltar medicinteknisk utrustning och system i frågor kring PDL och dess tillämpning.
- Att komma med förslag på begrepp och termer för de olika informationsnivåer som enligt LfMT behöver definieras för att kunna hantera data som genereras från medicinteknisk utrustning på ett patient- och informationssäkert sätt.
- Att komma med förslag på arbetssätt som på ett ändamålsenligt sätt tillgodoser kraven i gällande regelverk.

8 Mål

Inom ramen för syftet ovan har arbetsgruppen konkretiserat och haft som mål att försöka besvara följande frågeställningar:

- När är eller blir information i medicintekniska system att betrakta som en journalhandling?
- När betraktas inte information i medicintekniska system som en journalhandling?
- Vilka tekniska krav ställs på ett medicintekniskt system om systemet hanterar journalhandlingar isolerat från vårdgivarens ordinära journalsystem?
- Vilka krav förutsätter man att ett medicintekniskt system ska uppfylla om journalhandlingar som lagras i detta system nås via uthoppsintegrationer från vårdgivarens ordinära journalsystem?
- Vilka krav ställs på ett medicintekniskt system om journalhandlingar produceras i det medicintekniska systemet och därefter exporteras ut till vårdgivarens ordinära journalsystem, men där originalet av journalhandlingen finns kvar i det medicintekniska systemet?
- Vilka krav ställs på ett medicintekniskt system om journalhandlingar produceras i det medicintekniska systemet och därefter exporteras ut till vårdgivarens ordinära journalsystem, samtidigt som det raderas från det medicintekniska systemet?
- Vilka riktlinjer gäller för hur systemförvaltaren av det medicintekniska systemet ska förhålla sig om flera vårdgivare och/eller vårdenheter ska använda samma medicintekniska system och om data i det medicintekniska systemet är att betrakta som journalhandling?
- Vad gäller för regler för personal anställd av vårdgivaren som saknar vårdrelation till de patienter som finns registrerade i det aktuella systemet, t.ex. medicintekniker och IT-personal, och som behöver åtkomst till systemet i samband med användarsupport och servicearbete?

- Vad gäller för regler för extern personal, från t.ex. leverantör, som behöver åtkomst till det medicintekniska systemet i samband med användarsupport och servicearbete?
- Hur ska patientuppgifter som inte klassas som journalhandling hanteras i medicintekniska system?

Arbetsgruppen har även fått i uppgift att ta fram och formulera:

- Rekommendationer på hur man kan arbeta lokalt och tillsammans med leverantörerna för att säkerställa att implementeringen av det medicintekniska systemet följer PDL i tillämpliga delar.

9 Genomförande

Projektgruppen startade under januari 2014 och har sedan dess haft återkommande arbetsmöten kompletterade med fortlöpande korrespondens via e-post. Gruppen har också involverat övriga medlemmar i SI-nätverket i arbetet. Som huvudsakligt underlag för utredningsarbetet har projektgruppen utnyttjat lagar, förordningar och föreskrifter som berör de aktuella frågeställningarna. Gruppen har också tagit del av slutbetänkandet från utredningen om rätt information i vård och omsorg (SOU 2014:23).

10 Avgränsningar

Föreliggande rapport avser att ge vägledning och stöd för lokala bedömningar och beslut ute i respektive sjukvårdsförvaltning, men inte presentera explicita tekniska lösningar för hur specifika medicintekniska utrustningar och system ska implementeras och hanteras.

B. Lagrum och omvärldsanalys

11 Allmänt

Det medicintekniska regelverket regleras EU:s medicintekniska direktiv (MDD 93/42/EEC) om patientens rättighet till skydd av liv och hälsa vid användning av medicintekniska produkter (MTP). Sverige har, som EU-land konkretiserat MDD i svensk Lag om MTP (LMP).
Lagen har två huvudstråk:

- Tillverkarna åläggs att endast tillverka MTP lämpliga för avsedd medicinsk användning.
- Vårdgivarna åläggs att endast använda MTP lämpliga för patientens vårdsituation.

Sverige har starka traditioner vad gäller att skydda individers integritet och personuppgifter och går internationellt före inom detta område som regleras av Personuppgiftslagen (PUL). Patientdatalagen (PDL) är en förstärkning av individens skydd av personuppgifter som patient inom hälso- och sjukvården samtidigt som man vill öppna upp för möjligheten att, via sjukvårdens IT-system, dela patientuppgifter mellan olika vårdenheter och vårdgivare. PUL riktar sig till både industrin och landsting/regioner medan PDL i huvudsak riktar sig till vårdgivarna.

Underliggande regelverk beskrivs översiktligt i bilaga 2.

12 Socialdepartementet

Regeringen beslutade den 15 december 2011 att tillsätta en särskild utredare för att utreda och lämna förslag till en mer sammanhållen och ändamålsenlig informationshantering inom respektive och mellan hälso- och sjukvården och socialtjänsten. Utgångspunkten för uppdraget var att, efter en avvägning mellan verksamheternas behov av information och skyddet för den enskildes personliga integritet, kartlägga vilken typ av information som bedöms vara nödvändig att behandla. Utredningen kan betraktas som grundlig genomlysning av hur väl PDL är anpassad för och fungerar i vårdverksamheten.

Utredningen om rätt information i vård och omsorg (SOU 2014:23) föreslår i sitt slutbetänkande *”Rätt information i rätt tid för rätt användare”* en ny Hälso- och sjukvårdsdatalag och en ny Socialtjänstdatalag, vilka bör träda i kraft den 1 januari 2016. När den nya Hälso- och sjukvårdsdatalagen träder i kraft ska PDL upphöra att gälla. Följdändringar måste göras i flera andra lagar. Noterbart är att LMP inte är med bland de lagar som räknas upp.

Utredningen konstaterar att den information som behövs för att en individ ska få en god vård och omsorg inte alltid finns tillhands. Den uttalade målsättningen har varit att skapa förutsättningar för en informationshantering som bidrar till ännu bättre resultat för individer som är i behov av hälso- och sjukvård. ***Rätt information i rätt tid för rätt användare*** är en nyckel till vårdpersonalens möjligheter att göra ett bra arbete för den enskilde. Uppenbart är att informationshanteringen bör vara anpassad till det konkreta arbetet i vården.

Detta förutsätter att både dokumenterandet och utbytet av information mellan de som arbetar i verksamheten fungerar på ett *ändamålsenligt* sätt. Utredarna pekar på att det inte råder någon

tvekan om att komplexiteten i hälso- och sjukvården ökar, bland annat i takt med nya medicinska landvinningar och utvecklingen av nya läkemedel samt inte minst medicintekniska produkter. Samtidigt är nya möjligheter ofta förknippande med nya risker, exempelvis i form av otillräckligt skydd för den personliga integriteten. Det behöver därför göras en ständig avvägning mellan informationshanteringens nytta och risk.

Utredningen föreslår bl.a. att patienten inte har rätt att spärra uppgifter om ordinerade läkemedel, ordinationsorsak, läkemedlets namn, form, mängd, dosering, administrationssätt och tidpunkter för administrering.

PDL har inga uttryckliga krav på vårdgivarna att se till att vårddokumentationen är tillgänglig och användbar, eller att informationssystemen som används i verksamheten ska vara ändamålsenliga. Utredningen bedömer att integritetsskyddet behöver anpassas för att på bästa sätt skydda patientens integritet och möjliggöra god vård och omsorg.

Några av huvudpunkterna i förslaget till den nya Hälso- och sjukvårdsdatalagen är:

- Lagen syftar till att främja en informationshantering som tillgodoser god kvalitet, patientsäkerhet och kostnadseffektivitet.
- Vårdgivare ska se till att dokumenterade personuppgifter hanteras och förvaras så att obehöriga inte får tillgång till dem.
- Vårdgivare ska se till att de informationssystem som innehåller personuppgifter är lätta att använda, stödjer det kliniska arbetet, underlättar arbetet med kvalitetsutveckling, underlättar samverkan och utbyte av uppgifter mellan olika vårdgivare samt är utformade på sådant sätt att patienternas integritetsskydd tillgodoses.

Några av lagförslagets konsekvenser är:

- Informationshanteringen ska bli mindre beroende av hur vård och omsorg är organiserade och istället utgå från individen och individens behov.
- För den enskilde yrkesutövaren ska det endast vara tillåtet att ta del av uppgifter om han eller hon behöver uppgifterna för sitt arbete och om uppgifterna ska användas för något av de ändamål som är tillåtna enligt lagen.
- Behörigheten ska anpassas och begränsas till vad som behövs. Vårdgivare ska göra aktiva och individuella behörighetstilldelningar och för sammanhållen journalföring skall bedömningen vila på en riskanalys.
- Konsekvenserna av utformningen av behörigheten måste beaktas både ur patientsäkerhetsaspekter och ur aspekten att skydda patientens integritet.

Se bilaga 3 för en sammanfattning av Socialdepartementets utredning om rätt information i vård och omsorg (SOU 2014:23); *”Rätt information i rätt tid för rätt användare”.*

13 Synpunkter från myndigheter

13.1 Läkemedelsverket

I samtal med Enhetschef Medicinteknik Helena Dzojic framkom att det, enligt Läkemedelsverket (LV), inte råder något motsatsförhållande mellan krav på att skydda patienten från fysisk skada och skydd av patientens integritet. Båda skydden bör av tillverkaren utformas så bra som möjligt utan att de inverkar negativt på varandra. Tillverkaren har huvudansvaret att utforma MTP och dess anvisningar så att patienten ges skydd för liv och hälsa. Detta skydd ska riskhanteras av tillverkaren så länge som MTP används i vårdverksamheten. Vårdgivaren ska följa tillverkarens anvisningar och stödja tillverkarens riskhantering genom att via ”*Medical Devices Vigilance System*” tillhandahålla såväl nödvändig information som inblandad MTP när allvarliga avvikelser uppstår i den avsedda användningen.

Läkemedelsverket har tagit fram skriften *”Medicinska informationssystem – vägledning för klassificering av programvaror med medicinskt syfte”*. I denna publikation utreder man frågeställningen när en programvara är att anse som en MTP och vad det får för konsekvenser. Skriften finns att tillgå via länken http://www.lakemedelsverket.se/alla-nyheter/nyheter-2012/ny-vagledning-for-medicinska-informationssystem/

För mer detaljerad information om integritetsskydd i hälso- och sjukvården och hur det berör medicintekniska produkter hänvisade Helena till det arbete som pågår mellan Myndigheten för Samhällsskydd och Beredskap (MSB), Datainspektionen (DI) och LV.

13.2 Datainspektionen

Enligt Magnus Bergström, IT-säkerhetsspecialist på DI, är DI tillsynsmyndighet enligt PUL och då personuppgifter behandlas enligt PDL.

Han påpekar vidare att ”För Datainspektionens vidkommande saknar begreppet journalhandling betydelse för patientdatalagens tillämplighet och för hur patientuppgifter får hanteras i och kring medicintekniska produkter”. Han påpekar också att samma krav är tillämpliga vid behandling av personuppgifter enligt PDL, oavsett om de ingår i eller är att betrakta som en journalhandling eller inte. Begreppen *journalhandling* och *patientjournal* är ur DI:s perspektiv alltså inte avgörande för om eller när PDL är tillämplig.

Frågor som om och när information som hanteras i en MTP ska betraktas som journalhandling eller inte saknar därför, enligt honom, mening för DI:s tillsynsverksamhet.

14 Europeiska kommissionens (EC) samråd om mHälsa

Europeiska kommissionens (EC) rapport från samråd om mHälsa leder till ökande krav på säkerhet på mobila H&S-applikationer.

Se länk http://ec.europa.eu/digital-agenda/en/news/mhealth-europe-preparing-ground-consultation-results-published-today

Utdrag, fritt översatt från engelska till svenska ur Europeiska Kommissionens rapport januari 2015 om ” Public consultation on the Green Paper on mobile Health”:

Det inkom 211 separata svar från offentliga myndigheter, vårdgivare, patientorganisationer och webbföretagare, inom och utanför EU, på EC:s inbjudan till samråd om mHälsa. De gav sin syn på EC:s elva frågor om användningen av mHealth inom EU.

Nästan hälften (97) av de svarande anser att det behövs starkare integritet och säkerhetsverktyg (t.ex. datakryptering och autentiseringsmekanismer) för att stärka användarnas förtroende. Hälften av de svarande efterlyste en förstärkning av regelverket för både informationssäkerhet i mHälsa och för mHälsoprodukter. Nästan hälften av de tillfrågade begära en ökad tydlighet om patientsäkerhet i användning av mHälsa. Gärna med hjälp av certifieringssystem eller märkning av produkter för livsstils-, kvalitet- och välbefinnande appar. Några varnar dock för riskerna för en överreglering.

Webbföretagare anser att det är svårt att få tillgång till marknaden på grund av avsaknaden av ett tydligt regelverk, interoperabilitet och gemensamma kvalitetskriterier.

Av de som responderade anser 71 att prestanda- och säkerhetskrav samt ansvarsregler för livsstils- och välbefinnande-appar bör förtydligas genom lagstiftning, självreglering eller vägledning.

En femtedel av de som lämnade in svar anser att mer evidens behövs för att påvisa nyttan av mHälsa och dess kostnadseffektivitet. Av svaren hänvisade 21 till särskilda studier och projekt som har visat på effektivitetsvinster. Till exempel, enligt en studie, har försök i Norden visat att mHälsa skulle kunna generera en minskning på 50-60% av antalet vårdnätter på sjukhus och minska antalet återinläggningar av patienter med kronisk obstruktiv lungsjukdom. Samma studie uppskattar att mHealth kan minska de totala utgifterna för äldreomsorg med 25%.

Respondenterna föreslog:

- Att EU tillsammans med nationella åtgärder bör säkerställa kompatibilitet mellan mHälsa och elektroniska patientjournaler. Syftet är att skapa kontinuitet i den direkta vården av patienter vården och underlag för forskningsändamål.
- Att större vikt bör läggas på åtgärder för att främja öppna standarder och användning av gemensam öppen arkitektur eller öppna ”Application Programming Interface”.
- Att vårdpersonal, vårdgivare och användare bör delta aktivt i utvecklingen av lösningar för mHälsa.

Nästa steg är att EC under 2015 kommer att diskutera frågan med berörda om utformningen av regelverken för mHälsa. Frågan kommer också att lyftas som en av huvudpunkterna på ”eHealth Week” i Riga, maj 2015.

15 ECRI Institute

Vad kan gå fel på sjukhus? Många saker enligt ECRI Institute, en oberoende ideell USA-baserad organisation som bedriver forskning i syfte att hitta de bästa medicinska metoderna, utrustningarna, läkemedlen och vårdprocesserna för att förbättra patientvården. Risker orsakade av medicinsk teknik är ett bra exempel, eftersom risker kan leda till olyckor och patientskador. För att hjälpa sjukhusen att minska teknikrelaterade risker, publicerar ECRI institutet en årlig förteckning över *”Top 10 Health Technology Hazards”*.

Riskerna på listan för 2015 är:

1. Alarm Hazards: Inadequate Alarm Configuration Policies and Practices.
2. **Data Integrity: Incorrect or Missing Data in EHRs and Other Health IT Systems.**
3. Mix-Up of IV Lines Leading to Misadministration of Drugs and Solutions.
4. Inadequate Reprocessing of Endoscopes and Surgical Instruments.
5. Ventilator Disconnections Not Caught because of Mis-set or Missed Alarms.
6. Patient-Handling Device Use Errors and Device Failures.
7. “Dose Creep”: Unnoticed Variations in Diagnostic Radiation Exposures.
8. Robotic Surgery: Complications due to Insufficient Training.
9. Cybersecurity: Insufficient Protections for Medical Devices and Systems.
10. Overwhelmed Recall and Safety-Alert Management Programs.

För att ladda ner rapporten gratis besök www.ecri.org/2015hazards

15.1 Risk nr 2: Dataintegritet: Felaktiga eller saknade data i elektroniska patientjournaler och andra hälso- IT-system

Utdrag, fritt översatt från engelska till svenska, ur ECRI:s rapport från 2015 om Data Integrity: Incorrect or Missing Data in EHRs and Other Health IT.

Många beslut i dagens sjukvård är baserade på data i en elektronisk patientjournal eller annat IT-baserat medicinskt informationssystem (MIS). När dessa system fungerar väl får vårdpersonalen den information som de behöver för att ta lämpliga beslut om vård och behandling När fel uppstår eller fel finns i form av ofullständiga, felaktiga eller ”out-of-date”-information kan det leda till felaktiga beslut om behandling med patientskador som följd. Vad som gör detta problem så oroande är att dataintegriteten i MIS kan äventyras på ett antal olika sätt. När fel uppstår kan de dessutom vara svåra att upptäcka och korrigera.

Exempel på fel med avseende på dataintegritet:

- Patientuppgifter registreras i en annan patients register
- Uppgift saknas eller fördröjda dataleverans (t.ex., på grund av begränsningar i nätverket, konfigurationsfel eller förseningar i datainmatning)
- Klock-/synkroniseringsfel mellan olika medicintekniska produkter och system
- Standardvärden eller fält som förprogrammerats med felaktiga uppgifter används av misstag
- Inkonsekvenser i patientinformation när både pappers- och elektroniska journaler används parallellt

- Inaktuell information kopieras och klistras in i ett nytt register

Rekommendationer
Innan ett nytt system driftsätts eller ett befintligt modifieras, bör man beskriva processen för det kliniska arbetsflödet. Detta underlättar förståelsen av hur systemet fungerar eller kommer att användas av vårdpersonal. Identifiera ineffektivitet samt eventuella felkällor. Om t ex data kommer att flöda automatiskt mellan olika MIS och/eller medicintekniska system ska man ha kontroll på processerna för att upprätta en förbindelser från enheten till patientjournalen (association), för att bryta förbindelser mellan enheten och patienten när patienten mätdata inhämtas töms eller när patienten kopplas bort från enheten (dissociation). Det är viktigt att klinisk personal granskar uppgifterna innan de sparas i patientjournalen (validering).

Noggrant testa MIS, MTP-system och tillhörande gränssnitt för att kontrollera att systemet fungerar ordentligt och beter sig som förväntat. Detta gäller både införandet samt efter eventuella systemändringar. Var noga med att inkludera vårdpersonal i testprocessen.

Upprätta ett omfattande utbildningsprogram som leder till att användarna kan visa sin kompetens innan de får använda MIS/MTP-systemet. Skapa arenor för slutanvändare att söka hjälp (t.ex. enkel tillgång till superanvändare) när man arbetar med ett nytt system eller en ny funktion.

Etablera vägar att rapportera och utreda MIS-relaterade avvikelser, olyckstillbud och risker inom organisationen, samt till ECRI-institutet och andra berörda organisationer. Involvera ett multidisciplinärt team, inklusive Medicinsk Teknik och IT-personal, i samband med granskningen av avvikelserna.

C. MT-säkerhet och integritetsskydd

16 Allmänt

Lagen om medicintekniska produkter (LMP) är tydlig med att tillverkaren ska tillverka ändamålsenliga medicintekniska produkter (MTP) för avsedd användning och att användarna ska följa tillverkarnas anvisningar för att säkerställa ett optimalt skydd för patientens liv och hälsa. Patienters säkerhet ska vidmakthållas via riskhantering hos både tillverkare och användare genom hela produktens livscykel. Patientens integritetsskydd preciseras inte tydligt i denna lag.

Patientdatalagen (PDL) definierar uttrycket ”*Journalhandling*” som: *”Framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel och som upprättas eller inkommer i samband med vården av en patient och som innehåller uppgifter om patientens hälsotillstånd eller andra personliga förhållanden eller om vidtagna eller planerade vårdåtgärder”*. Information som inte är en journalhandling preciseras under punkten om ändamål med personuppgiftsbehandlingen i 2 kap. 4 § i PDL. Där omnämns inte information i form av mätdata från MTP, utöver det som ska journalföras som undersökningsresultat.

PDL anger att Personuppgiftslagen (PUL) gäller vid sådan behandling av personuppgifter inom hälso- och sjukvården som är helt eller delvis automatiserad eller där uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier, om inte annat följer av denna lag eller föreskrifter som meddelats med stöd av denna lag (1 kap. 4 §).

EU:s medicintekniska direktiv (MDD) uppdaterades år 2010 med att fristående programvaror för medicinsk användning ingår i definitionen av MTP. IT-baserade journalsystem och övriga former av medicinska informationssystem (MIS) regleras numera av det medicintekniska regelverket. Observeras bör att själva informationen om patienten, i alla dess former, inte är en MTP.

17 Patientsäkerhet vs Patientintegritet

Det gemensamma syftet med regelverken kring MTP är att till patienten tillhandahålla både fysisk och etisk säkerhet. Både tillverkaren av MTP och vårdgivaren ska vidta de åtgärder som behövs för att förebygga att patienter inte drabbas av vårdskador och att patienters integritet respekteras vid avsedd medicinsk användning av produkten.

Problem uppstår när skydd mot både vårdskada respektive skydd av patientintegritet suboptimeras. Detta kan skapa ineffektiv vård, som i sin värsta form kan innebära en ökad risk för vårdskada och i sin näst värsta form att patientens integritet skadas.

Exempel 1

Stark autentisering med hjälp av SITHS-kort eller SMS-tjänst för åtkomst till information på en övervakningsanläggning på hjärtintensiven (HIA). Om det vid larm om hjärtsvikt inte går att

logga in, p.g.a. tekniska problem eller frånvaro av nödvändigt SITHS-kort, vilket leder till att personuppgiften om vilken patient det är som larmar och aktuellt EKG från denne inte finns tillgängliga, så kan det innebära en mycket stor vårdskada där patienten i värsta fall avlider.

Exempel 2

Att inte använda någon form av behörighetsstyrning av vem som tar del av vilken patient som ligger inne på HIA och dennes aktuella hjärtstatus, kan innebära att obehörig ges åtkomst till informationen och kan sprida den via t.ex. sociala medier typ Facebook.

Problemformulering 1

Hur skall vi från ett medicintekniskt perspektiv tolka regelverket om skydd av patientens integritet för att uppnå:

1. ***Effektiv vårdverksamhet?***
2. ***Ändamålsenlig teknik och information för medicinskt bruk?***
3. ***Skydd mot otillbörlig användning av person-/patientuppgifter?***

Problemformulering 2

Hur skall uthopp från journalsystem till en MTP med lagrade MT-data hanteras?

MT-data som är väsentliga för god vård definieras som undersökningsresultat och ska därmed journalföras. Det sker antingen via manuell inskrivning eller som uthopp från patientens journal till en MTP. Manuellt inskrivna undersökningsresultat följer väl regelverket för journalföring.

Problemformulering 3

Hur skall regelverket tolkas när det gäller att spara eller förstöra MT-data?

MT-data produceras i mycket stora mängder och är i varierande grad försedda med artefakter. MT-data som inte anses som väsentlig för god vård förstörs löpande eller när så anses lämpligt automatiskt eller av vårdpersonalen. En journalhandling ska enligt PDL bevaras minst tio år efter det att den sista uppgiften fördes in i handlingen. Det krävs utredning och beslut hos IVO innan en journalanteckning kan förstöras. Det gäller för både ordinära och sekundära journalsystem.

Problemformulering 4

Hur ska regelverket tolkas när det gäller sekundärjournal?

För att hantera en stor och till omfattningen ökande mängd detaljerande uppgifter om en patient i en specifik vårdsituation upprättar medicinska specialiteter egna IT-system. Dessa IT-system är ofta, via olika gränssnitt, anslutna till olika medicinska utrustningar. Syftet är att både att skapa en effektiv hantering i den dagliga verksamheten och att inte belasta den ordinära journalen med stora datamängder, vilka kan skymma vital journalinformation (läsaren av journalen ”ser inte skogen på grund av alla träd”). Dessa IT-system är att betrakta som en sekundärjournal. Överföring av väsentlig information från dem till den ordinära journalen sker som regel i form av:

- Skriftliga utlåtanden från laboratoriemedicinska verksamheter som Röntgen, Kemlab m.fl.
- Skriftliga sammanfattningar från vårdenheter, exempelvis intensivvård
- Hänvisning via uthopp från den ordinära journalen till databaser som EKG, medicinska bildsystem m.fl.

Den patientansvariga läkaren, som normalt tar del av information i den ordinära journalen, har många gånger svårigheter att tillfullo förstå innebörden av den detaljrika informationen i sekundärjournaler. Denne är beroende av specialistläkarens bedömning av informationen och utlåtande för att kunna ställa den i förhållande till den vårdsituation som han/hon har att hantera. Allt fler medicinska specialiteter som Operation, Förlossning, Lungmedicin m.fl. upprättar numera egna sekundärjournaler.

17.1 Resonemang

Regelverkets anvisningar för att uppnå ändamålsenlig teknik och information för medicinskt bruk samt skydd mot otillbörlig användning vilar på två motsatser; underlätta och förhindra. Tillverkare och vårdgivare skall underlätta för användaren att göra rätt i avsedd medicinsk användning och samtidigt förhindra otillbörlig åtkomst av person-/patientuppgifter.

Underlätta

Från regelverket kan vi få anvisningar som underlättar för verksamheten att skapa en säker och effektiv vårdverksamhet enligt följande:

- **Patientsäkerhetslag** (SFS 2010:659) (PSL) ålägger vårdgivaren att bedriva ett systematiskt patientsäkerhetsarbete för att förebygga att patienter drabbas av vårdskador. Vårdgivaren skall utreda händelser i verksamheten som har medfört eller hade kunnat medföra en vårdskada, samt om möjligt eliminera eller åtminstone begränsa underliggande orsaker till vårdskada.
- **Lag om medicintekniska produkter** (SFS 1993:584) (LMP) är allmänna bestämmelser om medicintekniska produkter. Kravet på en medicinteknisk produkt är att den ska vara lämplig för sin användning.
- **Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården** (SOSFS 2008:1) anger att Verksamhetschefen ska ansvara för att endast säkra och medicinskt ändamålsenliga medicintekniska produkter och, till dessa, anslutna informationssystem används på patienter.
- **Personuppgiftslag** (SFS 1998:204) (PUL) ålägger vårdgivaren att enbart behandla personuppgifter som är adekvata och relevanta i förhållande till ändamålen med behandlingen och att personuppgifter inte bevaras under en längre tid än vad som är nödvändigt. Känsliga personuppgifter får behandlas för hälso- och sjukvårdsändamål, om behandlingen är nödvändig för medicinska diagnoser, vård eller behandling.

Förhindra

Från regelverken kan vi få anvisningar om att förhindra otillbörlig åtkomst av person-/patientuppgifter:

- **Patientdatalagen** (SFS 2008:355) (PDL) ålägger legitimerad vårdpersonal skyldighet att föra patientjournal. En patientjournal ska innehålla de uppgifter som behövs för en god och säker vård av patienten. Personuppgifter ska utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras. Den som arbetar hos en vårdgivare får ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården. Vårdgivare ska bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet ska begränsas till vad

som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. En vårdgivare ska se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och kan kontrolleras.

- **Personuppgiftslagen** (SFS 1998:204) (PUL) har som övergripande syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Den personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en lämplig säkerhetsnivå.

17.2 Konklusion

Regelverket är tydligt med att patientsäkerheten skall säkerställas, utöver en säkert konstruerad MTP, via från tillverkaren medföljande dokumenterade anvisningar, specifikationer och instruktioner för definierad avsedd medicinsk användning. Ansvarig tillverkare skall dessutom följa upp hur produkten används och vilka effekter den ger. Detta omfattar både den tekniska produkten och MT-data som genereras, dock inte informationen i sig.

En patientjournal skall endast innehålla de uppgifter som behövs för en god och säker vård av patienten. Det handlar om väsentliga uppgifter om bakgrunden till vård som patenten har erhållit.

Vi kan därmed konstatera att det finns ett utrymme mellan avsedd medicinsk användning i lag om MTP och dokumenterad journalanteckning för god och säker vård enligt PDL. I detta utrymme hanteras mängder med tekniskt genererad information från MTP. Det saknas idag en term och definition för denna informationsmängd. I denna utredning benämner vi den ***MT-data***, vilket avser en tekniskt genererad (insamlad/bearbetad) information från medicinteknisk produkt av biologiska (d.v.s. anatomiska, fysiologiska, kemiska, mikrobiologiska etc.) mätdata och/eller avbildningar från en patient (d.v.s. personuppgifter i form av mätdata), vilka ännu ej av legitimerad vårdpersonal bedömts vara autentiska och väsentliga för patientens diagnostik eller vård och därmed föremål att journalföras i patientens ordinära journal.

MT-data är känsliga personuppgifter som behandlas för hälso- och sjukvårdsändamål, där behandlingen är nödvändig för medicinska diagnoser, vård eller behandling. Vi anser att MT-data är lämplig att hanteras i enlighet med PUL. När information plockas ut, från flödet av MT-data, för väsentlig och avsedd användning blir informationen föremål för frågeställningen om den skall journalföras eller ej. Den journalförs om den bedöms som väsentlig för fortsatt god vård. När informationen behövs, används och dokumenteras i en patientjournal blir den en patientuppgift och skall därmed hanteras i enlighet med PDL.

Följande förkortningar används för att underlätta läsningen av våra konklusioner nedan avseende ovanstående problemformuleringarna:

- **LMP** Lag om medicintekniska produkter (SFS 1993:584)
- **PUL** Personuppgiftslagen (SFS 1998:204)
- **PDL** Patientdatalagen (SFS 2008:355)
- **PSL** Patientsäkerhetslagen (SFS 2010:659)
- **SI** SI-nätverkets arbetsgrupp som tagit fram denna rapport

Konklusion avseende problemformulering 1
Hur tolka regelverket om skydd av patientens integritet för att uppnå:

1. Effektiv vårdverksamhet
PUL: Personuppgifter får behandlas bara om den registrerade har lämnat sitt samtycke till behandlingen. I övrigt ges inga riktlinjer om effektivitet.

LMP: CE-märkt MTP har krav på sig att vara ändamålsenlig och därmed effektiv i sin avsedda medicinska användning.

SI: Vår bedömning är att när en medicinsk åtgärd påbörjas så har patienten samtidigt gett sitt samtycke till hanteringen av de personuppgifter som skapas, organisationen och den tekniska miljö som den hanteras i. Det är viktigt att behörighetssystem för CE-märkt MTP är ändamålsenliga och därmed effektiva i sin avsedda medicinska användning.

2. Ändamålsenlig teknik och information för medicinskt bruk
LMP: Kraven på en MTP är att den ska vara lämplig för sin avsedda medicinska användning.

SI: Vår bedömning är att utformningen av åtkomsten av information måste vara lämplig för sin avsedda användning. Huvudansvaret för det ligger på tillverkaren som i sin riskanalys skall ta ställning till både vad otillgänglig information innebär för patientsäkerheten samt vad risk för spridning av MT-data innebär för patientens integritet. Vårdgivaren skall å sin sida se till att det sammanhang som MTP används i är effektivt utformat så att man undanröjer risken för både patientskada och spridning av personuppgifter till obehöriga, samt att metoder, rutiner och användning sker av utbildad personal med behörighet för uppgiften. Behörigheten kan tilldelas antingen manuellt eller via elektronisk behörighet till MTP.

3. Skydd mot otillbörlig användning av person-/patientuppgifter
PUL: Vårdgivarens personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig.

SI: Vår bedömning är att den personuppgiftsansvarige i enlighet med PSL måste bygga vidare på MTP-tillverkarens riskanalys i syfte att förhindra vårdskador. Val av lämplig säkerhetsnivå för skydd av patientens integritet skall därmed ske i dialog med tillverkaren. Lämpligtvis sker det under upphandling av MTP. För befintlig MTP i klinisk användning bör vårdgivaren tillsammans med tillverkaren se över befintlig säkerhetsnivå för skydd av patientens integritet och, när så är erforderligt, höja den. Tillverkaren bär enligt LMP huvudansvaret att i sin riskanalys försäkra sig om att en höjning av säkerhetsnivån för skydd av patientens integritet inte ökar risken för vårdskador. Vårdgivaren är enligt både PUL och PDL ansvarig för att skydda de person-/patientuppgifter som vårdgivaren behandlar. Vårdgivaren är ansvarig för att endast använda ändamålsenliga MTP. Detta ansvar omfattar också utformningen av integritetsskydd så att det är ändamålsenligt.

Konklusion avseende problemformulering 2
Hur skall uthopp från ett PDL-anpassat journalsystem till en MTP med lagrade MT-data hanteras?
SI: För att vidmakthålla journalsystemets säkerhetsnivå så bör tillverkaren av MTP som tillåter uthopp från journalsystem till sin MTP se till att man via uthopp inte kan ta del av någon annan patients MT-data än för den patient i journalsystemet som uthoppet sker ifrån. Uthoppsintegrationen ska vara insynsskyddad så att dataströmmen inte obehörigen kan avlyssnas (krav enbart där IT-nätverket är definierat som öppet).

En mycket viktig del för att detta ska kunna säkerställas är att tillverkaren av MTP byggt in en funktion för att registrera patienternas personuppgifter (namn, personnummer etc.) och att detta görs på ett säkert sätt, samt att manuell registrering undviks.

Konklusion avseende problemformulering 3
Hur skall regelverket tolkas när det gäller att förstöra MT-data?
SI: MT-data är att betrakta som en personuppgift som lyder under PUL. Anvisningarna i lagen är tydliga med att personuppgifter inte skall bevaras längre tid än vad som är nödvändigt. Det stämmer väl överens med nuvarande praxis i hälso- och sjukvården. Undantag är om MT-data skall betraktas som journalhandling i form av undersökningsresultat. I detta fall måste dessa sparas i minst 10 år efter att den genererats eller ändrats.

Konklusion avseende problemformulering 4
Hur ska regelverket tolkas när det gäller sekundärjournal?
SI: Det finns en tradition inom medicinska serviceenheter (röntgen-, fysiologiska avdelningar och övriga laboratorieverksamheter) att lagra och spara undersökningsresultat i separata IT-system som över tid är skilda från vårdgivarens ordinära journal. MTP och MT-data som genereras av dessa betraktas ofta som en integrerad del i dessa separata IT-system. Dessa sekundärjournalsystem ska hanteras i enlighet med de krav som PDL och PUL ställer på hantering av personuppgifter. För t.ex. röntgenbilder har det sedan länge funnits riktade anvisningar från myndigheter om hur de skall hanteras. Vad vi känner till finns det inte motsvarande anvisningar för nya typer av sekundärjournaler med t.ex. personuppgifter om spirometriska funktioner m.fl. Generellt gäller att den tillverkare som sätter en sekundärjournal på marknaden skall hantera den i enlighet med det medicintekniska regelverket. Tillverkaren eller dennes återförsäljare har ansvaret att se till att det svenska regelverket följs och att produktens anvisningar är tillfyllest. Vårdgivaren ska alltid erhålla adekvata anvisningar från tillverkaren och efterfråga förtydligande information från tillverkaren när anvisningarna är undermåliga eller saknas.

Mot bakgrund av ovanstående resonemang är vår bedömning:

- Att när tillverkaren tydligt anger att då den avsedda användningen för deras MTP är för ordinarie eller sekundär journalföring så ska patientuppgifter i aktuell MTP hanteras enligt PDL.
- Att då det medicinska utlåtandet eller sammanfattningen enbart är att betrakta som en journalhandling, så hanteras utlåtandet, i enlighet med PDL som en journalhandling i den ordinära journalen. Det är vårdpersonalens ansvar att se till att journalhandlingen är tillfyllest. Underliggande information, t.ex. pedagogiskt stöd till utlåtandet, i MTP/MT-system hanteras

däremot i enlighet med PUL. Ytterst innebär det att informationen i MTP/MT-system kan förstöras löpande när den ej längre har betydelse i vårdsituationen.
- Att data i medicinska databaser och MTP/MT-system, där det inte finns någon uttalad anvisning om att personuppgiften är en journalhandling, hanteras enligt PUL.

18 Spärrad information och konsekvenser av begränsad tillgång till MT-data

Vid analysen av nyttan med tillgång till information relaterat till risk för ökat integritetsintrång måste särskild hänsyn tas till att MT-data är en informationsmängd som i många fall är jämförbar med information om patientens aktuella läkemedelsordinering, vilken generellt sett är särskilt viktig för patientens liv och hälsa.

Behörig personals tillgång till MT-data kan i princip begränsas på två sätt:
- Aktiv handling begränsar tillgången till MT-data
  - Patient begär spärr av journalinformation på vårdenhet, vilket inkluderar registrerad MT-data som normalt görs tillgänglig via den ordinära journalen
  - Lokalt behörighetssystem integrerat i MTP
- Ofrivilligt hinder som innebär en helt eller delvis begränsad åtkomst till MT-data
  - Bortglömda eller felaktiga inloggningsuppgifter
  - Kort med certifikat finns inte tillgängligt när det behövs vid inloggning
  - Felfunktion hos MTP som förhindrar åtkomst

PDL inrymmer ingen möjlighet för patienten att exklusivt spärra specifika informationsmängder på en vårdenhet, exempelvis MT-data. Vi i arbetsgruppen känner inte till något fall där patienten begärt spärr av sin journalinformation p.g.a. att denne vill integritetsskydda registrerad MT-data. Däremot känner vi till fall där MT-data varit spärrad vilket har skapat medicinska komplikationer i en akut vårdsituation.

Exempel

Patient begärde spärr på journaluppgifter registrerade på vårdenhet A. Patienten hade där ett EKG registrerat. En tid senare uppstod en akut situation och patienten ankom till vårdenhet B där personal hade kännedom om att patienten hade ett EKG registrerat på vårdenhet A. EKG på enhet A ansågs väsentlig i den aktuella situationen. Då journalsystemet inte hade teknisk möjlighet att temporärt häva denna spärr, trots patientens godkännande, föranledde detta att EKG:t, på enhet A, förblev otillgängligt.

Det är relativt vanligt med tillverkare som har ett behörighetssystem integrerat med sin MTP. Exempel på detta finns i system för radiologi, ögonbottenbilder och spirometri. Det är inte helt ovanligt att system med behörighetsinloggning i praktiken utestänger personal som formellt har behörighet att komma åt nödvändig information, vilken behövs för att ge en god vård till patienten. Detta innebär för hälso- och sjukvården att vi har skapat en mångfald av olika verksamhetssystem med olika behörighetssystem och säkerhetsnivåer, med och utan central styrning av tilldelade rättigheter.

Tillverkaren ska i sin riskanalys, som grund till CE-märkningen, beakta konsekvenserna för patienten vad oönskad otillgänglighet till medicinsk information innebär i risk för patientens säkerhet. Detta ska balanseras mot allt för lättillgänglig MT-data och vilken risk det innebär för patientens integritet, vilket det medicintekniska regelverket ger knapphändig information om.

Enligt MDD så ska tillverkares MTP och anvisningar till användarna ständigt riskhanteras så att de ständigt förbättras via utvärderingar av användandet och inrapporterade avvikelser.

I Sverige hanteras säkerhetstjänster om autentisering, patientens medgivande och spärr av information, direkt eller indirekt, centralt av Inera (http://www.inera.se/). De koordinerar landstingens och regionernas gemensamma e-hälsoarbete och utvecklar tjänster till nytta för invånare, vård- och omsorgspersonal och beslutsfattare. Att få tillverkarna av MTP att bygga in tekniska lösningar som är kopplade till Ineras tjänster är inte rimligt. Sverige är en liten marknad som i huvudsak importerar den MTP som används i vården. Det finns inte så många tillverkare av journalsystem och de har bättre förutsättningar att kan koppla dessa säkerhetstjänster till sina produkter. Det finns också en större betalningsvilja hos landstingen att ta en extra kostnader för att PDL-anpassa några få system än att öka kostnaderna för alla MTP.

Tillgång till aktuell MT-data är ofta avgörande i vårdögonblicket. Som exempel så kan det vara information från övervakningsutrustning på intensivvårdsplatser, eller EKG från tidigare undersökningar. Det kan finnas skäl att överväga om viss information alltid behövs, som en nödvändig förutsättning, för att ge patienten en god och säker vård. Vi anser att det finns goda grunder att rekommendera en riskanalys på de MTP där Vårdgivaren har för avsikt att använda en annan teknisk lösning för inloggning, än den tillverkaren av aktuell MTP föreskriver.

Via vårdgivarens riskanalys så kan behörigheten anpassas till vårdgivarens intentioner. Viktigt är att all förändring av tillverkarens anvisade behörighetsskydd sker i dialog med tillverkaren, så att vårdgivaren får full vetskap om eventuella konsekvenser som en förändring av behörighetsskyddet innebär. Konsekvenserna av utformningen av behörighetsskyddet beaktas därmed både ur patientsäkerhetsaspekter och ur aspekten att skydda patientens integritet.

D. Resultat

19 Allmänt

Information från en medicinteknisk produkt (MTP) ska finnas tillgänglig när den behövs i patientens vårdsituation. Patientens integritet ska samtidigt skyddas i tillräcklig omfattning, utan att förhindra eller försämra den vård som patienten är i behov av.

Patientdatalagen (PDL) definierar uttrycket ”*journalhandling*” som: *”Framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel och som upprättas eller inkommer i samband med vården av en patient och som innehåller uppgifter om patientens hälsotillstånd eller andra personliga förhållanden eller om vidtagna eller planerade vårdåtgärder”*.

Vi i arbetsgruppen anser att det finns en övertolkning av PDL:s definition av uttrycket journalhandling. En personuppgift bör inte definieras som en journalhandling utifrån den tekniska miljön som den hanteras i, utan av om ansvarig vårdpersonal bedömer att informationen är väsentlig för patientens vård och behandling. När personuppgiften bedöms som väsentlig så utgör den en journalhandling och ska journalföras i patientens ordinära journal i enlighet med PDL. En journalhandling ska bevaras i minst 10 år och får förstöras efter beslut av IVO.

Personuppgifter i vården som inte journalförs i patientens ordinära journal och därmed inte lyder under PDL hanteras av PUL. Informationen ska förstöras löpande när den ej längre behövs, utifrån det behov som förelåg när togs fram.

Det är inte rimligt att få tillverkarna av MTP att bygga in tekniska lösningar som är kopplade till Ineras säkerhetstjänster om autentisering, patientens medgivande och spärr av information. Sverige är en liten marknad som i huvudsak importerar den MTP som används i vården. Vår bedömning är att hanteringen av dessa tjänster måste ske i eller via MTP där tillverkarens avsedda användning är att hantera patienters journaler.

Det hade underlättat om regelverket för informationshantering harmoniseras med regelverket för MTP. Bäst vore om EU-direktivet MDD försågs med ett avsnitt som hanterade all informationshantering, inklusive journalföring. Så att det sker på ett, för alla parter ändamålsenligt vis, så att både patientens skydd mot vårdskador och kränkning av integritet tillgodoses.

20 När anses information genererad från medicinteknisk utrustning vara en journalhandling

Socialstyrelsens handbok till SOSFS 2008:14, som tydliggör myndighetens föreskrifter avseende informationshantering och journalföring, är ett stöd till vårdverksamheten avseende journalföring. Här framgår att en journalhandling är patientuppgifter som upprättas eller inkommer i samband med vården av en patient och som innehåller uppgifter om patientens hälsotillstånd eller om andra personliga förhållanden eller om vidtagna eller planerade vårdåtgärder. En eller flera journaluppgifter utgör en journalanteckning. En eller flera journalanteckningar utgör en

journalhandling. En eller flera journalhandlingar utgör patientjournalen. Enligt PDL 3 kap. 6 § ska patientjournalen innehålla väsentliga uppgifter som behövs för en god och säker vård av patienten. Om uppgifterna finns tillgängliga, ska en patientjournal alltid innehålla:

1. Uppgift om patientens identitet
2. Väsentliga uppgifter om bakgrund till vården
3. Uppgift om ställd diagnos och anledning till mera betydande åtgärder
4. Väsentliga uppgifter om vidtagna och planerade åtgärder
5. Uppgift om den information som lämnats till patienten och om de ställningstagande som gjorts i fråga om val av behandlingsalternativ och möjligheten till en förnyad medicinsk bedömning

Patientjournalen ska vidare innehålla uppgift om vem som har gjort en viss anteckning i journalen och när anteckningen gjordes. En patientjournal får endast innehålla de uppgifter som behövs för den vård och administration av patienter. Den bör i förekommande fall innehålla:

1. Uppgifter om aktuellt hälsotillstånd,
2. Uppgifter om ordinationer av t.ex. läkemedel och olika behandlingar,
3. Uppgifter om förskrivningsorsak vid ordination av läkemedel,
4. Undersökningsresultat
5. Uppgifter om överkänslighet för läkemedel eller vissa ämnen,
6. Uppgifter om vårdhygienisk smitta, samt
7. Epikris och andra sammanfattningar av genomförd vård.

Med hjälp av olika medicintekniska utrustningar skaffar sig vårdgivaren en möjlighet att fånga data som beskriver patientens hälsotillstånd. Användaren av den medicintekniska utrustningen kan utifrån hela eller delar av detta informationsflöde av mätdata, som vi i denna rapport benämner till MT-data, fatta beslut kring fortsatt vård och behandling av den enskilde patienten. MT-data som bedöms som autentiska och väsentliga för god vård definieras som undersökningsresultat och ska därmed journalföras.

Noterbart är att det inte är självklart att all MT-data har en väsentlig betydelse för den fortsatta vården av patienten. MT-data som inte har en väsentlig betydelse ska därmed inte heller betraktas eller hanteras som journalhandling.

Det är därför viktigt att det finns framtagna riktlinjer i verksamheten för vad som skall betraktas som ett relevant undersökningsresultat, så att enbart sådana uppgifter sparas till den ordinära eller sekundära journalen. Observera att det är vanligt i sekundära journalsystem typ laboratoriesystem att icke granskade undersökningsresultat blandas med granskade resultat som bedöms som väsentliga för patientens fortsatta vård. I dessa system är det än viktigare med tydliga riktlinjer.

Personuppgift som inte anses utgöra en patientuppgift regleras av PUL. Kriteriet för detta är huruvida uppgiften kan knytas direkt eller indirekt till en fysisk person.

20.1 Konklusion

Information (MT-data) om en patient som är genererad av en MTP blir en journalhandling när legitimerad vårdpersonal har bedömt informationen som autentisk och väsentlig för god vård eller i den fortsatta behandlingen av patienten och dokumenterat den i patientens ordinära journal. Man kan förenklat formulera det som att vårdpersonalen ”tillverkar” en journalhandling av MT-data.

21 Tekniska krav på medicinteknisk utrustning med hänsyn till patientdatalagen

21.1 Utrustningar och system utan teknisk koppling till den ordinära journalföringen

Denna kategori utgörs av utrustningar och system där personuppgifter behandlas helt separat från den ordinära journalföringen, men där hela eller delar av dessa uppgifter är väsentliga för fortsatt vård och behandling och därmed ska klassas som patientuppgifter, vilka ska journalföras manuellt i den ordinära journalen. I de fall där man inte överför några MT-data utan i den ordinära journalen hänvisar till uppgifter som finns registrerade i ett MT-system, betraktas detta system som en sekundärjournal, vilket, enligt vår bedömning ovan i avsnitt 16.2, ”Problemformulering 4”, i tillämpliga delar ska följa PDL.

21.1.1 Tekniska krav beroende på användares organisationstillhörighet

Var MTU används	Stark autentisering	Insynsskydd Kryptering	Behörighet	PDL-loggning	Aktivt val	Patientens begärda spärrar	Samtycke
Inom en vårdenhet	Ja	Ja	Ja	Ja	Nej	Nej	Nej
Inom en vårdgivare	Ja	Ja	Ja	Ja	Ja	Ja	Nej
Sammanhållen journalföring (mellan vårdgivare)	Ja	Ja	Ja	Ja	Ja	Ja	Ja

För förklaring av rubriker se avsnitt 27.4 Bilaga 4,”Ordlista”.

PDL-loggning: (Utdrag ur SOSFS 2008:14 11 §)
Vårdgivaren ska ansvara för att det i ledningssystemet finns rutiner som säkerställer att:

1. Det av dokumentationen av åtkomsten (loggarna) framgår vilka åtgärder som har vidtagits med patientuppgifterna,
2. Det av loggarna framgår vid vilken vårdenhet och vid vilken tidpunkt åtgärderna har vidtagits,
3. Användarens och patientens identitet framgår av loggarna,
4. Systematiska och återkommande stickprovskontroller av loggarna görs,
5. Genomförda kontroller av loggarna dokumenteras, och
6. Loggarna sparas i minst tio år.

Vad vi i arbetsgruppen känner till finns det inga dokumenterade krav där vårdgivaren systematiskt ska kontrollera loggar hos MTP. Däremot så gäller generellt att vid misstanke om missbruk eller obehörig åtkomst så ska Vårdgivaren kontrollera loggarna hos MTP. Tillverkaren av MTP är ansvarig för konstruktion och anvisningar om användning av MTP:s loggar.

21.1.2 Undantag

Om utrustningen eller systemet används på ett IT-nätverk som inte definieras som ett ”Öppet nät” finns inget krav på Stark autentisering eller kryptering av datatrafiken.

Exakt vad som definierar ett ”Öppet nät” är oklart, men Datainspektionen har i ett yttrande påpekat att ett IT-nätverk dit fler än ett personuppgiftsombud har tillgång bör betraktas som ett öppet nät (Ref: Svar på fråga till Datainspektionen ställd av Värmlands Läns Landsting) Klart är att Internet och Sjunet är öppna nät.

Varje landsting eller region ansvarar för att definiera sitt eller sina lokala IT-nätverk (SS-EN-80001-1).

21.1.3 Personnummerhantering

För att upprätthålla ett korrekt personuppgiftsregister måste den medicintekniska utrustningen hantera personnummer enligt svensk standard för folkbokföring av fysiska personers identitetsbeteckning. Bestämmelser om personnummer finns i 18 § Folkbokföringslagen (1991:481). Där anges att personnummer ska lagras med en 12-tecken lång serie utan bindestreck. Personnummer kan dock presenteras med 10 tecken plus bindestreck om så önskas. För att säkerställa en korrekt registrering av personuppgifter ska man undvika manuell inmatning av dessa.

21.1.4 Bevarande av journalhandlingar

Generellt sett gäller att journalhandlingar ska bevaras i minst 10 år efter det att sista uppgiften förts in till handlingen. Regeringen eller den myndighet som regeringen bestämmer får meddela förskrifter om att vissa slags journalhandlingar ska bevaras längre än 10 år. Vårdgivaren ansvarar för att journalhandlingarna förvaras på ett sådant sätt att de är läsbara fram till dess att de får gallras. (Se även avsnitt 27.2 Bilaga 2 – ”Underliggande regelverk”).

21.1.5 Utrustningar och system integrerade med den ordinära journalföringen

Denna kategori utgörs av MTP och MTP-system som är integrerade med den ordinära journalföringen. Denna integration implementeras huvudsakligen via ”Uthoppsintegration”

respektive ”Överföringsintegration” samt dessa båda i kombination, fortsättningsvis benämnt *hybridintegration*.

Då dessa MTP och MTP-system hanterar personuppgifter kommer de att regleras under PUL. Den som är personuppgiftsansvarig hos vårdgivaren måste därför vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna. Vanligtvis görs en lämplighetsbedömning för varje register utifrån hur känsliga uppgifterna är och nödvändiga säkerhetsåtgärder vidtas därefter.

21.1.6 Uthoppsintegration

Användare når journalhandlingar lagrade i den medicintekniska utrustningen eller systemet via den ordinära journalföringen. Om användaren enbart kan nå lagrade journalhandlingar via detta uthopp, bör journalsystemet där uthoppet sker från hantera de tekniska krav som definieras i avsnitt 20.1.1. Om så är fallet kvarstår följande krav på utrustningen eller systemet dit uthoppet sker:

- Enbart anropad persons patientuppgift presenteras.
- Funktioner för vidare sökning på andra personer är nedlåsta och inte möjligt att utföra.
- System dit uthopp sker måste vara uppbyggda med en korrekt organisationsstruktur (önskvärt att HSA används). Detta krävs bland annat för att den ordinära journalen ska kunna hantera patientens begärda spärrar eller andra funktioner kring aktivt val.
- Bevarande av journalhandlingar sker enligt PDL 3 kap. 17 §.
- Åtkomst till lagrade journalhandlingar i annat syfte än vård av enskilda patienter måste föregås av en godkänd autentiseringsmetod enligt PUL.
- Säker och korrekt personnummerhantering. En primärkälla för personnummer bör finnas.
- Journalhandlingar måste vara lagrade med information om vilken vårdgivare, vårdenhet och legitimerad yrkesutövare (eller person med särskilt förordnade) som skapat och ansvarar för handlingen, samt tidpunkt om när den upprättats.
- Vårdgivaren ska kunna uppfylla kravet om logg av när, hur och för vem patientdata visats för vårdpersonal. Åtkomstloggning bör ingå i det system dit uthopp sker, även om uthoppet loggas från det ordinära journalsystemet.
- Om de tekniska kraven (enligt avsnitt 20.1.1) inte kan säkerställas i uthoppet, måste detta säkerställas i den utrustning eller system dit uthoppet görs.

Exempel på områden där uthoppsintegrationer från den ordinära journalen används:

- EKG
- Labsvar
- Röntgenbilder
- Ögonbottenbilder
- Ultraljudsbilder

21.1.7 Överföringsintegration

MT-data som anses vara väsentliga för vidare vård av enskilda patienter överförs till den ordinära journalföringen från den medicintekniska utrustningen eller systemet. Om kommunikationen mellan de producerande utrustningarna eller system och den primära journalföringen sker över ett öppet nätverk så ska trafiken mellan dessa vara åtkomstskyddad. Det åligger sedan det

ordinära journalsystem som tar emot MT-data att säkerställa att dessa hanteras så att PDL följs. MT-data som är relevant att journalföra men inte överförs p.g.a. tekniska hinder måste manuellt skrivas in i den ordinära journalen. Viktigt att observera är att det måste finnas en utpekad vårdperson, med en vårdrelation med patienten, som står för journalhandlingens riktighet. Originalinformationen kan tillåtas ligga kvar i MTP/MTP-systemet och hanteras då enligt PUL.

Exempel på områden där MT-data överförs till den ordinära journalen:

- Obstetriska mätdata
- PDF-export (t.ex. en slutrapport)
- Stråldos

21.1.8 Kombination av uthopps- och överföringsintegration (Hybridintegration)

Användare når personuppgifter som är väsentliga för fortsatt vård och behandling av enskilda patienter via en kombination av två integrationer mot MTP/MTP-systemet.

Kravet på dessa utrustningar och system blir därmed en kombination av de som nämns under dessa båda integrationstyper med avseende på det aktuella bidraget från var och en av dem.

Exempel på områden där hybridintegrationer används:

- Hantering av ultraljudsinformation inom obstetrik
- Remiss och svar inom fysiologi och radiologi

22 Riktlinjer till förvaltare av medicintekniska utrustningar och system

Förvaltare av medicintekniska produkter och system ska säkerställa:

- Att MTP korrekt installerade enligt tillverkarens anvisningar
- Att MTP är lämplig för avsedd medicinsk användning
- Att MTP följer Vårdgivarens policy om informationssäkerhet för MTP
- Att behörighetssystemet är anpassat till det medicinska ändamålet
- Att en riskanalys, gärna i samverkan med tillverkaren, föregår installation av behörighetssystem som inte följer tillverkarens av MTPs anvisningar
- Att personregister, när sådant upprättas i MTP, är anmält till vårdgivarens personuppgiftsombud
- Att rutiner, enligt tillverkarens anvisningar, finns för systematiskt underhåll av MTP och anslutna IT-system inklusive backup av personregister
- Att rutiner finns för hur vårdpersonalen journalför MT-data i patientens ordinarie journal
- Att kommunikation med överföring av patientuppgifter och integration av MTP med journalsystem sker på ett sådant sätt att ingen obehörig kan ta del av uppgifterna
- Att användaren har nödvändig kunskap om användning av systemet
- Att användaren har tilldelats behörighet
- Att Verksamhetschefen har godkänt MTP med anslutna IT-system för användning i vårdverksamheten **innan** första användningstillfället på patient

En medicinteknisk produkt ska vara lämplig för sin användning.
Produkten är lämplig när den:

- Är rätt levererad och installerad samt underhålls och används i enlighet med tillverkarens märkning, bruksanvisning eller marknadsföring, och
- Uppnår de prestanda som tillverkaren avsett och tillgodoser höga krav på skydd för liv, personlig säkerhet och hälsa hos patienter, användare och andra.

Informationssäkerhetspolicyn ska säkerställa att:

- Patientuppgifter i vårdgivarens dokumentation är åtkomliga och användbara för den som är behörig (tillgänglighet),
- Patientuppgifterna är oförvanskade (riktighet),
- Obehöriga inte ska kunna ta del av patientuppgifterna (sekretess), och
- Det i sådana informationssystem som är helt eller delvis automatiserade är möjligt att i efterhand entydigt kunna härleda åtgärder till en identifierad användare (spårbarhet).

Personuppgiftsombud är en person, ofta en anställd, som ser till att personuppgifter behandlas korrekt och lagligt inom en verksamhet. Ombudet ska föra en förteckning över register och annan behandling av personuppgifter och hjälper registrerade att få felaktiga uppgifter rättade.

22.1 Checklista för att säkerställa en korrekt hantering av personuppgifter

Checklistan nedan (bifogas även som bilaga 1) är ett hjälpmedel som tagits fram av arbetsgruppen till hjälp för förvaltare av medicintekniska utrustningar och system med syfte att stödja hanteringen av personuppgifter i MTP i enlighet med gällande regelverk.

1. Grunden i en korrekt hantering av personuppgifter i MTP är att det som ska mätas, bearbetas etc. sker med medicinsk teknik som är lämplig för sitt ändamål. Det är viktigt att detta är verifierat med tillverkaren av aktuell MTP. – Lagrum LMP
2. Avseende MTP som enbart visar MT-data i avidentifierad form, ska användaren vara medveten om att det är upp till dem själva att fånga och koppla väsentlig information till aktuell patient för journalföring. – Lagrum LMP och PDL
3. Visas MT-data pseudonymiserat, t.ex. ”Patient sängplats 4:2”, så ska nyckeln som kopplar pseudonym med patient-ID vara försedd med skydd mot otillbörlig åtkomst. För de som får åtkomst till nyckeln gäller punkt 7 nedan. – Lagrum LMP och PUL
4. Det behövs ett ändamålsenligt behörighetssystem till varje enskild eller system av MTP. Det innebär att behörighetssystemet inte hindrar den vårdpersonal som behöver få omedelbar åtkomst till information när den behövs, samtidigt som patientens integritetsskydd är så starkt som det är möjligt utifrån vårdsituationen. Behörighetssystemet kan vara manuellt och dokumenterat på papper eller elektroniskt implementerat i aktuell MTP. – Lagrum LMP och PUL
5. Patientens identitet ska på ett säkert vis fastställas och verifieras när ID kopplas till MT-data som härrör från aktuell patient. – Lagrum LMP och PUL

6. Lagras MT-data med patient-ID, oberoende av var detta sker, så ska personregistret anmälas till vårdgivarens personuppgiftsombud. – Lagrum PUL
7. Visas MT-data med patient-ID så ska det säkerställas att endast behörig personal, med spårbarhet (manuellt eller elektroniskt) avseende vem, när och vad, tar del av MT-data. – Lagrum LMP och PUL
8. MT-data får förstöras löpande när den inte längre behövs. – Lagrum PUL
9. Sker en bearbetning av MT-data, så ska metoden verifieras mot MTP-tillverkarens anvisningar. – Lagrum LMP
10. När vårdpersonal bedömer att MT-data är väsentlig att journalföras, så ska det ske enligt fastställda lokala riktlinjer om hur och när MT-data definieras som undersökningsresultat, samt genom integration göras pedagogiskt tillgänglig som stöd till journalhandlingen. – Lagrum PDL
11. Undersökningsresultat bör journalföras i MTP vilken av tillverkaren är avsedd för att användas för att journalföra patientuppgifter. – Lagrum LMP och PDL
12. När man integrerar MT-data från MTP via IT-nätverk med journalsystem, så skall man vara säker på om överföringen av patientuppgifter sker via ett öppet eller slutet nät och skapa förbindelsen säkerhetsmässigt utifrån dessa förutsättningar. – Lagrum LMP och PDL
13. Om integrationen mellan MTP och journalsystem sker via ett öppet nät, så ska överföring av patientuppgifter görs på ett sådant sätt att ingen obehörig kan ta del av uppgifterna, och åtkomst till patientuppgifter ska om möjligt regleras via stark autentisering. – Lagrum LMP och PDL
14. Integreras MT-data med journalsystem via integrationsmjukvara, ska man verifiera med tillverkaren av journalsystemet om lämpliga kriterier för avsedd användning för uthopps-, överföring- eller hybridintegration finns implementerade. – Lagrum LMP, PUL och PDL
15. Omfattningen av vilken åtkomst till journalsystemet som ska tillåtas ska föregås av ett beslut av verksamhetschef om åtkomst ska ges enbart inom en vårdenhet, inom vårdgivaren eller mellan flera vårdgivare. – Lagrum PDL
16. Det ska finnas praktiska rutiner framtagna för hur man spärrar patientuppgifter i de fall där patienten har en rättighet att införa en spärr. – Lagrum PDL
17. Det ska finnas praktiska rutiner framtagna för hur vårdgivaren inhämta och dokumenterar patientens samtycke för sammanhållen journalföring. – Lagrum PDL
18. Förstörande av patients journaluppgift lagrad i MIS får ske först efter beslut av IVO om vad och vilken information i journalhandlingen som får förstöras. – Lagrum PDL
19. När det uppstår osäkerhet om hur man ska hantera informationssäkerheten i en MTP/MIS p.g.a. att de olika regelverken inte korrelerar med varandra, bör man genomföra en ny riskanalys med tillverkarens riskhantering av aktuell MTP/MIS som grund. Syftet är att om möjligt minimera både risken för patienten att drabbas av vårdskada och risken för kränkning av sin integritet. – Lagrum PSL

20. Verksamhetschefen ska, **innan** användning på första patienten, godkänna att MTP med anslutna IT-system och behörighetssystem får användas på patient. – Lagrum LMT

22.2 Dialog med leverantörerna och exempel på samverkansfora

Svensk lagstiftning är unik i världen gällande sitt starka skydd för patientintegritet. Lagstiftaren kräver funktioner som i många fall måste utvecklas och implementeras unikt för den svenska marknaden, och som få eller inga andra länder efterfrågar i dagsläget. Att ställa dessa krav eller ge signaler i upphandlingar till presumtiva leverantörer är ett allt för trubbigt verktyg, vilket i sin tur antingen leder till att kraven marginaliseras i upphandlingsprocessen, eller att man får lika många olika varianter på tekniska lösningar som man har utrustningar och system.

Vi anser att ett mycket mer effektivt tillvägagångssätt är att diskutera krav kring behörighet, autentisering, loggning, aktivt val, samtycke och spärr i olika former av kundmöten, workshops och seminarier.

I detta sammanhang är de nätverk som redan finns, t ex SKL, MTF, Swedish Medtech m.fl. och de som håller på att formeras, viktiga fora för utbyte av idéer, diskussion och påverkan mellan leverantör och användare.

På användarsidan finns sedan 2011 ***3R*** som är ett nätverk bildat av de tre största regionerna i Sverige; Stockholms Läns Landsting, Västra Götalandsregionen och Region Skåne. Inom 3R konstaterar man att implementeringen av standarder skiljer sig mellan leverantörer och att någon form av samsyn behövs. Nätverket har hittills bl.a.:

- Identifierat IHE (se nedan) som en form för att testa och kvalitetssäkra informationsutbyte mellan enskilda MTP och system av MTP
- Tagit fram generisk text som börjat användas i upphandlingsunderlag
- Etablerat ett samarbete med Swedish Medtech

SI-nätverket är en växande nationell sammanslutning av personer inom sjukvården vilka arbetar som System Integrator (SI) (se SS-EN 60601-1 Appendix H 6.2) eller har motsvarande funktion hos sin respektive arbetsgivare. SI-nätverket är organisatoriskt knutet till LfMT. SI-nätverket har till syfte att knyta samman medlemmarnas gemensamma intressen inom området Medicinsk teknik och IT inom:

- Informationsutbyte mellan deltagande landsting/regioner
- Kravställning avseende IT infrastruktur
- Funktionella och regulatoriska krav på MT-system
- Integration mellan MTP och andra IT-stöd
- Implementering av IT-produkter i vården
- Riskhantering
- Upphandling och avtalsfrågor

IHE står för ***Integrating Healthcare Enterprise*** och kommer från USA. Nätverket, eller snarare konceptet, uppstod inom sjukvården och har sina rötter inom radiologin. IHE är idag ett gemensamt initiativ från vårdprofession och industri för att underlätta informationsdelning mellan

IT-system i vården. IHE främjar samordnad användning av etablerade standarder såsom DICOM och HL7 (se nedan) för att hantera specifika kliniska behov till stöd för vården och dess processer. IT-system som utvecklats i enlighet med IHE kommunicerar bättre med varandra, är enklare att implementera, och gör det därmed möjligt för vårdgivare att använda informationen på ett effektivare sätt. IHE är ingen egen standard, utan ett *standardiserat arbetssätt* med samverkan mellan vårdgivare och industri till gagn för båda parter.

HL7 står för ***Health Level Seven*** och är en internationell organisation som verkar för att skapa standarder för utbyte, hantering och integration av elektronisk hälsoinformation. HL7 är primärt inriktad mot klinisk och administrativ information och arbetar aktivt för att sprida användandet av standarder inom hälso- och sjukvård. Lokalt i Sverige finns HL7 Sweden som ser sig som ett forum för samarbete, diskussioner och erfarenhetsutbyte. Man interagerar med HL7 International och har också ett nära samarbete med SIS.

I sammanhanget kan till sist också nämnas ***Continua Health Alliance*** som är en global sammanslutning av företag verksamma inom medicinteknik, hälsovård och fitness som arbetar för interoperabilitet och standarder mellan personliga medicinska produkter. Inom Continua delar man upp det man gör i tre segment för att invånarna skall:

- Klara sig själva i sin egen hemmiljö längre
- Kunna hantera kroniska sjukdomar bättre själv och därmed underlätta för vårdgivare
- Försöka undvika sjukdomar genom aktiv friskvård

Leverantörerna bör i bättre utsträckning än idag instruera vårdgivaren hur deras utrustning ska implementeras för att säkerställa kraven i PDL. Det finns ett generellt behov av att förse MTP och dess medföljande anvisningar med mer information om hur och varför integritetsskyddet är utformat som det är.

Vårdgivarna och förvaltarna av dessa utrustningar och system bör också bli bättre på att definiera tekniska krav och styra leverantörerna i deras val av tekniska lösningar. Att ett system stödjer Stark Autentisering innebär inte per automatik att den tekniska lösningen ser likadan ut som för resten av de system som stödjer SITHS-kortinloggning. Arkitekturen kan skilja betänkligt och det är mycket upp till vårdgivaren att styra detta.

23 Risker och möjligheter

Nr.	Risk/Möjlighet	Åtgärd
1.	Leverantör av MTP vill inte anpassa sin produkt för att tillgodose nödvändiga funktioner för att stödja PDL.	I första hand val av annan produkt. I andra hand måste produkten installeras och bristerna hanteras på plats. Kan kräva resurser som ska vägas in i produktvalet.
2.	PDL-krav i upphandling kan innebära få eller inga anbud.	PDL-krav i upphandling kan i dagsläget troligen inte vara ”ska-krav”. Förutom att krav viktas rätt bör man redovisa att eventuella extra

		kostnader för lokal anpassning kommer vägas in vid utvärderingen.
3.	Effekter vid uppfyllande av PDL som innebär att åtkomstmöjligheten till journalhandlingarna blir omständlig.	Patientsäkerheten måste komma först. Krav för att uppfylla informationssäkerhet och spårbarhet får vägas mot detta. – Se slutbetänkandet från utredningen SOU 2014:23.
4.	Vårdpersonal vågar inte eller begränsar insamling av information från patienten, p.g.a. risken att dessa data automatiskt blir journalhandling.	Information till vårdpersonal om gällande lagstiftning och implementering av denna hos aktuell MTP.
5.	Funktion för loggning av vem som har haft tillgång till patientdata saknas i MTP.	I första hand via krav på leverantör i samband med upphandling. Kan även lösas då MTP integreras (via t.ex. uthoppsintegration) med primärsystem som kan säkerställa dessa tekniska krav.

24 Diskussion

Vi har under utredningens gång identifierat att det inom regelverket för hälso- och sjukvården finns två parallella världar för hantering av medicinteknisk säkerhet och informationssäkerhet; Det finns ett tydligt regelverk för MTP med EU-direktiv, svensk lag, förordningar från regering samt föreskrifter från myndigheterna Läkemedelsverket och Socialstyrelsen. Det finns också ett separat regelverk om medicinsk informationssäkerhet med svensk lag, föreskrifter från myndigheterna Socialstyrelsen och Datainspektionen. Dessa båda regelverk saknar en tydlig koppling eller hänvisning till varandra. Trots rådande faktum att journalsystem, vilka är klassade som en medicinteknisk produkt, hanterar merparten av den information som är av avgörande betydelse för diagnos och god vård.

Faktum är att den information som regelverket för informationssäkerhet reglerar i huvudsak hanteras i medicintekniska produkter eller system av dessa och att informationsdelningen över IT-nätverk mellan MTP sker i traditionella IT-produkter som är byggda för allmänt bruk, utan något uttalat syfte om medicinsk användning.

Det är först nere på standardiseringsnivå som vi kan hitta regler som tydligt kopplar samman de olika regelverken. Ett exempel på detta är standarden SS-EN 60601-1 *”Elektrisk utrustning för medicinskt bruk – Del 1: Allmänna fordringar beträffande säkerhet och väsentliga prestanda”.* I kapitel 14 om *”Programmerbara elektriska medicinska system”*, påpekas i fotnoten under 14.6.1 i standarden, *”Identifiering om kända och förutsägbara risker”*, att tillverkaren i sin riskhantering ska inkludera informationssäkerhet och brist på integritet i hanteringen av data.

Läkemedelsverkets *”Vägledning för medicinska informationssystem”* (LVFS 2014:7) berör ytligt integritetsproblematiken med hänvisning till gällande standarder:

- SS-EN ISO 27799:2008 *”Hälso- och sjukvårdsinformatik – Ledningssystem för informationssäkerhet i hälso- och sjukvården”*. Standarden är avsedd att hjälpa vårdgivare att säkerställa en lämplig lägsta säkerhetsnivå för att bibehålla konfidentialitet, riktighet och tillgänglighet för personuppgifter inom hälso- och sjukvården.
- SS-EN 80001-1 *”Riskhantering tillämpad på IT-nätverk innehållande medicintekniska produkter”*. Standarden riktar sig framför allt till vårdgivaren och är utformad som ett stöd då en medicinteknisk produkt har förvärvats av en vårdgivare och är tänkt att ingå i ett IT-nätverk.

Noterbart är att ingen information ges av Läkemedelverket till tillverkare av MTP om hur informationssäkerheten ska tillgodoses.

Vi noterar också att Socialdepartementets utredning om rätt information i vård och omsorg (SOU 2014:23), *”Rätt information i rätt tid för rätt användare”,* inte berör lagen om medicintekniska produkter och dess tillhörande författningar. Det närmaste de kommer i detta avseende är att de konstaterar att komplexiteten i hälso- och sjukvården ökar med utvecklingen av nya MTP och att det inte finns något motsatsförhållande mellan skydd mot patientskada och skydd av patientens integritet. Integritetsskyddet skall tillgodoses så långt det är möjligt utan risk för patientens liv och hälsa.

Trots det naturliga sambandet mellan regelverken för informationssäkerhet och medicintekniska produkter så integrerar de båda regelverken inte med varandra. Vad är de bakomliggande orsakerna till att de beter sig som ”olja i vatten”?

Vi i arbetsgruppen gör bedömningen att detta beror på respektive regelverks uppkomst och historik. Lagstiftarna har, sedan länge, insett att tillverkaren av medicintekniska produkter har kunskaper av betydelse om hur deras produkt skall konstrueras och användas för i möjligaste mån ge skydd av liv och hälsa. Denna insikt har tillverkarna accepterat och tar därmed ansvaret för produkten och dess anvisningar om avsedd medicinsk användning. Lagstiftare, vårdgivare och tillverkare är överens om grundprincipen att *tillverkaren* har huvudansvaret för säker användning av MTP.

Inom IT-området så finns det en motsatt historik. Tillverkarna av IT-produkter insåg tidigt att de *inte* kan ta ansvar för hur deras produkter används. Deras ansvar kan bara sträcka sig till att ange hur IT-miljön ska se ut för att deras IT-produkt skall fungera enligt specifikation. Tar man exemplet med Microsoft så kan de inte hantera sin mjukvara på något annat sätt mot bakgrund av den enormt snabba och stora spridning som deras operativsystem Windows fått. Användarna accepterade heller inte begränsningar från tillverkarna. När Microsoft av konkurrensskäl börja begränsa användarnas möjligheter att modifiera i koden och användningen av deras IT-produkter uppstod en ny och numera stor bransch av ”Open source” IT-produkter typ Linux. Lagstiftare, vårdgivare och tillverkare är överens om grundprincipen att *användarna* har huvudansvaret för användningen av IT-produkter.

Man kan diskutera om den medicinska information som MTP och IT-produkter hanterar ska följa regelverket för medicinsk teknik eller det för IT, eller om det behöver skapas ett helt nytt regelverk liknande Tryckfrihetsförordningen (SFS 1949:105). Hur ska personskada vägas mot kränkning av individens integritet och vilken hänsyn tas det i sin tur till medborgarnas rätt till allsidig upplysning samt tillgång till allmänna handlingar?

Vår bedömning är att det finns stora etiska frågeställningar som bakomliggande orsaker till att medicintekniska produkter, medicinsk information samt offentlighetsprincipen hanteras i separata regelverk. Vi inom arbetsgruppen har inte full insikt i alla etiska aspekter, utan överlåter till läsaren av denna rapport att själv~~a~~ fundera kring dessa. Arbetsgruppen har däremot stora erfarenheter av det medicintekniska regelverket och har dessutom tagit intryck av utredningen om rätt information i vård och omsorg (SOU 2014:23) från Socialdepartementet. Vi har kommit fram till att diskussionen om patientsäkerhet kontra patientintegritet vilar på följande grundläggande perspektiv:

1. Avsedd användning av medicinsk information
2. Ändamålsenlig utformning av åtkomst till medicinsk information
3. Patientens samtycke till hantering av medicinsk information inkluderas per automatik när denne tar emot vård
4. Effektivt nyttjande av medicinsk information i samband med vårdtillfället
5. Ansvar för innehåll i anvisningar till användarna av medicinsk information
6. Sammanhållen riskhantering avseende riskanalys och avvikelsehantering av risk för både patientskada och kränkning av patientens integritet

Man kan resonera kring vem som är ”tillverkare” av medicinsk information. Tydligt är dock att informationen är en personuppgift. Ägare av informationen är patienten som den medicinska informationen handlar om. MTP registrerar och hanterar MT-data, men ”tillverkar” den inte. Vårdpersonalen använder medicinsk information för medicinska ställningstaganden och åtgärder. Regelverket för journalföring är tydliga med att den legitimerade vårdpersonal som skriver en journalhandling ansvarar för den. Man skulle kunna benämna det som att de är ”tillverkare” av journalhandlingen.

Tillverkaren av MTP kan inte ta ansvar för patientens mätvärden. Deras ansvar sträcker sig till mätteknologin. Kvar ligger, hos den som tar del av mätvärdet, att tolka om mätresultatet är en artefakt eller ett rimligt värde och därmed ett autentiskt undersökningsresultat. Utifrån detta kan man resonera att när MT-data används i medicinskt syfte så ”tillverkas” en journaluppgift. Den yrkesmässiga bedömningen kvalitetssäkrar MT-data. Användaren kan ge MT-data en avsedd användning enbart för den patient som MT-data härstammar ifrån. Detta synsätt passar väl in i dagens evidensbaserade vård med medicinska riktlinjer.

Denna rapport försöker att bidra med att tydliggöra problematiken som finns i gråzonen mellan LMP och PDL, samt föreslå lösningar på denna problematik. Vårt fokus ligger på PDL och MTP. Det är dock många frågor som återstår att ta en dialog kring:

- Kan informationssäkerhet utformas utifrån avsedd användning av medicinsk information?
- Hur får vi till stånd en evidensbaserad medicinsk informationssäkerhet?
- Kan man tillämpa principerna från standarden SS-EN 80001-1: *”Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter”*? Den anvisar att

vårdgivaren skall utgå från tillverkarens riskhantering av MTP och bygga vidare med en egen riskhantering av IT-nätverk. Kan man lägga till en ny nivå avseende medicinsk information, d.v.s. att de som ansvarar för riktlinjer i vården också tar ansvar för informationssäkerheten?

- Alla aktörer vill att patienten skall erhålla erforderligt skydd så att denne inte blir skadad eller får sin integritet kränkt. Vem eller vilka bär huvudansvaret att avgöra vad erforderlig informationssäkerhet är? Ytterst har patientansvarig vårdpersonal ansvaret att se till att patienten inte skadas eller får sin integritet kränkt. Har de adekvata förutsättningar att ta beslut om vad som är erforderligt? Normen idag är att informationssäkerhetsexperter anser sig ha dessa förutsättningar. Ska det vara så?

25 Slutsatser

Utifrån uppdragets syfte och mål har arbetsgruppen formulerat följande slutsatser:

- Patienten har en rättighet att, när MTP används, erhålla en säker och ändamålsenligt god hälso- och sjukvård.

- Riskanalys ska ligga som grund för att minimera risken för patienten att bli skadad eller erhålla en försämrad vård eller få sin integritet kränkt.

- Det råder inte något motsatsförhållande mellan krav på att skydda patienten från fysisk skada och skydd av patientens integritet. Båda skydden bör tillverkaren av MTP utforma så bra som möjligt utan att de inverkar negativt på varandra.

- Att det i dagens regelverk existerar en gråzon mellan inhämtandet av biologiska mätdata från patienten och när dessa data definitionsmässigt enligt Patientdatalagen (PDL) är att betrakta som journalhandling.

- Att ett nytt begrepp ***MT-data*** införs, vilket av arbetsgruppen definieras som:
”Tekniskt genererad (insamlad/bearbetad) information från medicinteknisk produkt av biologiska (d.v.s. anatomiska, fysiologiska, kemiska, mikrobiologiska etc.) mätdata och/eller avbildningar från en patient (d.v.s. personuppgifter i form av mätdata), vilka ännu ej av legitimerad vårdpersonal bedömts vara autentiska och väsentliga för patientens diagnostik eller vård och därmed föremål att journalföras i patientens ordinära journal”.

- MT-data är att betrakta som en personuppgift som lyder under PUL. Anvisningarna i lagen är tydliga med att personuppgifter inte ska bevaras längre tid än vad som är nödvändigt. Detta stämmer väl överens med nuvarande praxis i hälso- och sjukvården.

- MT-data som klinisk personal bedömer vara autentisk och har betydelse för den enskilda patientens fortsatta vård och behandling ska anses utgöra journaluppgift/journalhandling och sparas i den ordinära journalen. Detta görs antingen genom att användaren skriver in detta manuellt i journalsystemet, via elektronisk överföring från MTP till journalsystem, eller via ett elektroniskt uthopp från journalsystemet till MTP.

- Vår bedömning är att när en medicinsk åtgärd påbörjas så har patienten samtidigt, underförstått, gett sitt samtycke till hanteringen av de personuppgifter som skapas, till organisationen och den tekniska miljö som informationen hanteras i.

- Utformning av åtkomst till informationen måste vara lämplig för sin avsedda användning. Huvudansvaret för detta ligger på tillverkaren som i sin riskanalys skall ta ställning till både vad otillgänglig information innebär för patientsäkerheten samt vad risk för spridning av MT-data innebär för patientens integritet.

- Vårdgivaren skall å sin sida se till att det sammanhang som MTP används i är adekvat utformat så att man undanröjer risken för både patientskada och att spridning av personuppgifter till obehöriga undanröjs eller minimeras. Dessutom skall vårdgivaren säkerställa att metoder och rutiner vid användning av MTP utförs av utbildad personal med behörighet för uppgiften. Behörigheten kan tilldelas både antingen manuellt eller via elektronisk behörighet till MTP.

- Uthopp som sker från journalsystem som regleras av PDL. För att vidmakthålla journalsystemets säkerhetsnivå, så bör tillverkaren av MTP som tillåter uthopp från journalsystem säkerställa att enbart den information som användare i journalsystemet har behörighet till exponeras och att nätverkstrafiken är insynsskyddad. Dessutom ställs särskilda krav på att MT-data som exponeras hålls beständig över tid i MTP enligt de gallringsbeslut som vårdgivaren satt upp för aktuell informationsmängd.

- Då MT-data överförs elektroniskt till journalsystem ska detta ske på ett sådant sett att informationen inte kan avlyssnas av obehöriga eller förvanskas på vägen. Det åligger sedan journalsystemet att hantera åtkomst och beständighetskrav med utgångspunkt från PDL. MT-data som ligger kvar i MTP regleras som en personuppgift enligt PUL.

- Om flera än en vårdgivare lagrar MT-data i en gemensam databas och där syftet är medicinsk uppföljning, måste informationen vara ”taggad” på ett sådant sätt att filtrering och åtkomst kan göras så att både PUL och PDL följs i avseende tillämpliga delar.

- Åtkomst till MT-data i annat syfte än vidare vård och behandling av enskild patient, t.ex. i samband med servicearbete, gäller de krav som förutsätts anges i PUL.

- Vårdgivarens personuppgiftsansvarige måste, i enlighet med PSL, bygga vidare på MTP-tillverkarens riskanalys om i syfte att förhindra vårdskador. Val av lämplig säkerhetsnivå för skydd av patientens integritet skall därmed ske i dialog med tillverkaren. Lämpligtvis sker detta under upphandling av MTP. För befintlig MTP i medicinsk användning bör vårdgivaren tillsammans tillverkaren se över befintlig säkerhetsnivå för skydd av patientens integritet och, när så är erforderligt, höja den.

- Tillverkaren bär enligt LMT huvudansvaret huvudansvaret för att i sin riskanalys försäkra sig om att en ökad säkerhetsnivå för skydd av patientens integritet inte samtidigt ökar risken för

vårdskador. Vårdgivaren är ansvarig enligt både PUL och PDL att skydda de person-/patientuppgifter som vårdgivaren behandlar.

26 Förslag till fortsatt arbete

Vi anser att dagens situation med tydliga skillnader mellan de regelverk som styr skyddet av patientens personliga integritet respektive patientsäkerheten ur ett tekniskt/fysiologiskt perspektiv i många avseenden är olycklig och frustrerande. Å andra sidan signalerar Socialdepartementets utredning om rätt information i vård och omsorg (SOU 2014:23), *”Rätt information i rätt tid för rätt användare”,* en intention från lagstiftaren att med patientnyttan i centrum förenkla regelverket med avseende på hanteringen av medicinsk information. Fortfarande saknar vi dock en tydlig koppling till LMP och dess tillhörande författningar.

För att effektivt kunna fortsätta arbeta att samordna regelverken och skapa en global samsyn blir samarbetet och nätverkandet mellan olika myndigheter, organisationer och intressegrupper inom och utom svensk sjukvård allt viktigare. Ingen part kan eller ska lösa problemen på egen hand – då skapas bara nya problem.

Vi kan notera att det finnas ett gemensamt intresse hos både leverantörer och vårdgivare att arbeta för standardiserade lösningar avseende skydd av patientens integritet. Det finns ett antal initiativ både inom och mellan respektive gruppering. Internationellt har nu informationssäkerhet i hälso- och sjukvården, bl.a. genom ECRI:s rapporter, hamnat i fokus. Ett problem som berörts ovan är dock att den svenska lagstiftningen är unik i världen vad gäller sitt starka skydd för patientintegritet. Detta faktum begränsar många gånger de lokala leverantörernas möjligheter att tillhandahålla system som till fullo uppfyller regelverket. De tillgängliga systemlösningarna i de MTP som marknadsförs i Sverige är ofta anpassade och riskhanterade utifrån internationell standard. Att för svenska förhållanden utveckla och kvalitetssäkra unika funktioner som få internationella marknader efterfrågar, är inte ekonomiskt intressant. Alternativet är att vårdgivaren (d.v.s. köparen) får bära en större del av kostnaden.

I detta sammanhang framstår en svensk anslutning till IHE-samarbetet som mer eller mindre oundviklig. Det är en global arena för att torgföra det svenska synsättet på patientens säkerhet och integritet i MTP och MIS. Både leverantör och vårdgivare kan dra nytta av IHE-standardisering.

Avseende förslaget från utredningen om rätt information i vård och omsorg (SOU 2014:23) avseende en ny hälso- och sjukvårdsdatalag, bör SKL driva frågan att den nya lagen relateras till LMP och dess tillhörande författningar. SKL bör också föreslå införandet av ett nytt begrepp *MT-data*, vilken, enligt vår uppfattning hanteras i enlighet med PUL.

Ur Socialdepartementets utredning om rätt information i vård och omsorg citerar vi: *”En närmare reglering som tar sikte på behörighetstilldelning ska finnas i författningar av lägre valör än lag”* (SOU 2014:23, sid 1128, tredje stycket). Vi rekommenderar därför att Läkemedelsverkets medicintekniska enhet får huvudansvaret att utforma författningen för behörighetstilldelning så att den stämmer överens med övriga författningar som reglerat MTP. Vi anser också att Läkemedelsverket bör få uppdraget att inom EU driva frågan om ett gemensamt regelverk för ändamålsenliga behörighetssystem för MTP.

I en alltmer ”uppkopplad” och ”distribuerad” värld med en utveckling av hemsjukvård, mobil diagnostik- och terapiutrustning och molnlagring av data som vi ännu bara sett början av, kommer efterhand helt nya frågeställningar och problem att komma på agendan för upprätthållande av patient- och informationssäkerheten. SI-nätverket kommer även i fortsättningen som en del i sitt uppdrag att för LfMT:s räkning bevaka vad som händer inom området medicinsk teknik och IT. Vi avser också att hålla en nära kontakt med vårt nybildade nationella ”systernätverk” för säkerhetssamordnare.

I syfte att presentera innehållet i denna rapport och därigenom sprida det till en vidare krets, samt för att starta en offentlig diskussion kring de frågeställningar rapporten tar fram, arrangerar LfMT en seminariedag den 25 mars 2015 i SKL-huset i Stockholm. Idén är också att till detta seminarium bjuda in föredragshållare som representerar de berörda intressesfärerna och låta dessa presentera sin syn på den aktuella situationen, samt mötas i en paneldiskussion.

Vårdgivarna bör, med denna rapport som utgångspunkt, utarbeta interna policies om informationssäkerhet för hantering av de MTP som finns inom respektive vårdgivares organisation.

Vi i arbetsgruppen har stora förhoppningar att denna rapport tillför berörda myndigheter en större insikt i frågan och att den påskyndar utvecklingen av regelverken för informationssäkerhet och MTP/MIS, så att svensk sjukvård får harmoniserade regelverk inom detta område.

E. Referenser

27 Referenser

- SFS 2010:677 - Lag om ändring i patientdatalagen (SFS 2008:355)
- SFS 2010:659 - Patientsäkerhetslag
- SFS 2008:355 - Patientdatalag
- SFS 1998:204 - Personuppgiftslag
- SFS 1993:584 - Lag om medicintekniska produkter
- SFS 1991:481 - Folkbokföringslag
- SFS 1985:125 - Tandvårdslag
- SFS 1982:763 - Hälso- och sjukvårdslag
- SFS 1949:105 - Tryckfrihetsförordning
- SOU 2014:23 - Rätt information på rätt plats i rätt tid (”Utredningen om rätt information i vård och omsorg”)
- SOU 2007:48 - Patientdata och läkemedel m.m.
- SOSFS 2008:14 - Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården
- SOSFS 2008:1 - Användning av medicintekniska produkter i hälso- och sjukvården
- LVFS 2014:7 - Vägledning för medicinska informationssystem
- LVFS 2003:11 – Läkemedelsverkets föreskrifter om medicintekniska produkter
- SS-EN ISO 14971:2012 - Medicintekniska produkter - Tillämpning av ett system för riskhantering för medicintekniska produkter
- SS-EN 80001-1:2011 - Riskhantering tillämpad på IT-nätverk innehållande medicintekniska produkter
- SS-EN ISO 27799:2008 - Hälso- och sjukvårdsinformatik - Ledningssystem för informationssäkerhet i hälso- och sjukvården
- SS-EN 60601-1:2006 - Elektrisk utrustning för medicinskt bruk
- http://www.continuaalliance.org
- http://www.datainspektionen.se/ordlista
- http://www.ihe.net
- http://www.ihe-europe.net
- http://www.inera.se/tjanster--projekt/siths
- http://www.ivo.se
- http://www.lakmedelsverket.se
- http://www.lfmt.se/si-forum.html
- http://www.socialstyrelsen.se/patientsakerhet/riskomraden/medicinteknik
- Bonniers svenska ordbok, 10:e upplagan
- LDC, Lunds universitet
- Nationalencyklopedin

F. Bilagor

28 Bilagor

28.1 Bilaga 1 Checklista för att säkerställa en korrekt hantering av personuppgifter

		Att hantera			Är hanterad	
Punkt	**Aktivitet**	**Ja**	**Nej**	**Åtgärd**	**OK**	**Lagrum**
1.	MTP mäter/ registrerar MT-data	X		Verifiera med tillverkaren att MTP är lämplig för sitt ändamål		LMT
2.	Visa MT-data avidentifierat			Verifiera med användarna att de själva måste fånga väsentlig information för journalföring		LMT, PDL
3.	Visa MT-data Pseudonymise-rad			Nyckel som kopplar pseudonym med patient-ID ska förses med skydd mot otillbörlig åtkomst. För de som får åtkomst gäller punkt 7.		LMT, PUL

4.	Åtkomst till MT-data	☐ ☐	Verifiera att behörighetssystem, manuell eller elektroniskt, är ändamålsenligt och tillfyllest för åtkomst till MT-data	☐	LMT, PUL
5.	Kopplar patient-ID till MT-data	☐ ☐	Patients identitet ska på ett säkert vis fastställas och verifieras	☐	LMT, PUL
6.	Lagra MT-data Med patient-ID	☐ ☐	Personregister anmälas till vårdgivarens personuppgiftsombud	☐	PUL
7.	Visa MT-data Med patient-ID	☐ ☐	Säkerställa att endast behörig personal med spårbarhet (manuellt eller elektroniskt) om vem som, tar del av MT-data	☐	LMT, PUL
8.	Förstörande av MT-data med eller utan patient-ID	☐ ☐	MT-data förstörs löpande När den inte längre behövs	☐	PUL
9.	Bearbetning av MT-data	☐ ☐	Verifiera metoden mot tillverkarens anvisningar	☐	LMT

10.	Vårdpersonals bedömning av MT-datas väsentlighet för journalföring	☐ ☐	Fastställ riktlinjer om hur och när MT-data blir undersökningsresultat som ska journalföras samt genom integration görs pedagogiskt tillgänglig som stöd till journalhandlingen	☐	PDL
11.	Journalföra Undersöknings-resultat	☐ ☐	Verifiera med tillverkaren Att MTP avsedda användning är att journalföra patientuppgifter	☐	LMT, PDL
12.	Integrera MT-data, via IT-nätverk, med journalsystem	☐ ☐	Kontrollera om över-föringen av patient-uppgifter sker via ett öppet eller slutet nät	☐	LMT, PDL
13.	Integration via öppet nät	☐ ☐	Överföring av patient-uppgifter görs på ett sådant sätt att ingen obehörig kan ta del av uppgifterna, och åtkomst till patientuppgifter föregås, om möjligt, med av stark autentisering	☐	LMT, PDL

14.	Integrera MT- data, via integrations-mjukvara, med journalsystem	☐ ☐	Verifiera med tillverkaren Om lämplig kriterier för uthopps-, överföring- eller hybridintegration	☐	LMT, PUL, PDL
15.	Åtkomst till journalsystemet	☐ ☐	Beslut om åtkoms ska ges enbart inom en vårdenhet, inom vårdgivaren eller mellan flera vårdgivare	☐	PDL
16.	När patienten har en rättighet att kunna spärra sin journal	☐ ☐	Ta fram praktiska rutiner om patientuppgifter spärras	☐	PDL
17.	När vårdgivaren har skyldighet att inhämta patientens samtycke för sammanhållen journalföring	☐ ☐	Ta fram praktiska rutiner Om hur samtycke dokumenteras och hanteras.	☐	PDL
18.	Förstörande av journaluppgift	☐ ☐	Efter beslut av IVO förstörs journal-handlingen	☐	PDL

19.	Regelverk för MTP och patients informations-säkerhet korrelerar inte med varandra	☐ ☐	Genomför en ny riskanalys, som bygger vidare på tillverkarens riskhantering av MTP, för att, om möjligt, minimera båda riskerna för patienten att drabbas av vårdskada eller kränkning av sin integritet	☐	Patient-säkerhetslag
20.	Innan användning, av MTP innan användning, av MTP eller MT-system, på den första patienten	☐ ☐	Verksamhetschefen har godkänt att MTP med anslutna IT-system och behörighetssystem får användas på patient	☐	LMT

28.2 Bilaga 2: Underliggande regelverk

28.2.1 Patientsäkerhetslagen (SFS 2010:659)

Patientsäkerhetslagen syftar till att främja en hög patientsäkerhet inom hälso- och sjukvård. I lagen finns bestämmelser om vårdgivarens skyldighet att bedriva ett systematiskt patientsäkerhetsarbete (3 kap.) och bestämmelser om behörighetsfrågor och legitimation för vårdpersonal (4 kap.). Lagen ålägger vårdgivaren att planera, leda och kontrollera verksamheten på ett sätt som leder till att kravet på god vård i Hälso- och sjukvårdslagen (SFS 1982:763) respektive Tandvårdslagen (SFS 1985:125) uppfylls. Vårdgivaren ska vidta de åtgärder som behövs för att förebygga att patienter drabbas av vårdskador. Vårdgivaren ska också utreda händelser i verksamheten som har medfört eller hade kunnat medföra en vårdskada. Syftet med utredningen ska vara att:

1. Så långt som möjligt klarlägga händelseförloppet och vilka faktorer som har påverkat det, samt
2. Ge underlag för beslut om åtgärder som ska ha till ändamål att hindra att liknande händelser inträffar på nytt, eller att begränsa effekterna av sådana händelser om de inte helt går att förhindra.

28.2.2 Lag om medicintekniska produkter (SFS 1993:584)

Lag om medicintekniska produkter är allmänna bestämmelser om medicintekniska produkter. Kravet på en medicinteknisk produkt är att den ska vara lämplig för sin användning. Produkten är lämplig när den:

1. Är rätt levererad och installerad samt underhålls och används i enlighet med tillverkarens märkning, bruksanvisning eller marknadsföring, och
2. Uppnår de prestanda som tillverkaren avsett och tillgodoser höga krav på skydd för liv, personlig säkerhet och hälsa hos patienter, användare och andra.

En medicinteknisk produkt får släppas ut på marknaden eller tas i bruk i Sverige endast om den uppfyller de krav och villkor som gäller för den. Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om väsentliga krav vid införsel av medicintekniska produkter.

28.2.3 Läkemedelsverkets föreskrift om medicintekniska produkter (LVFS 2003:11)

Läkemedelsverkets föreskrift om medicintekniska produkter anger att medicintekniska produkter måste uppfylla de väsentliga krav och som är tillämpliga på dem med hänsyn tagen till deras avsedda ändamål.

28.2.4 Socialstyrelsens föreskrift om användning av medicintekniska produkter i hälso- och sjukvården (SOSFS 2008:1)

Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården anger att verksamhetschefen ska ansvara för att endast säkra och medicinskt ändamålsenliga medicintekniska produkter och, till dessa, anslutna informationssystem används på patienter.

28.2.5 Svensk standard – Medicintekniska produkter – Tillämpning av ett system för riskhantering för medicintekniska produkter (SS-EN ISO 14971:2012)

Standarden om tillämpning av ett system för riskhantering för medicintekniska produkter hjälper tillverkare av medicintekniska produkter att uppfylla väsentliga krav i Läkemedelsverkets

föreskrifter (LVFS 2003:11) om medicintekniska produkter. Den hjälper också tillverkaren att uppskatta, beräkna och bedöma riskerna hos sina produkter, kontrollera dessa risker, samt att övervaka riskhanteringens effektivitet. Kraven i standarden är tillämpliga på alla stadier i livscykeln för en medicinteknisk produkt.

28.2.6 Svensk standard för elektrisk utrustning för medicinskt bruk (SS-EN 60601)

Standard för elektrisk utrustning för medicinskt bruk behandlar grundläggande säkerhet (både fysisk och i viss mån etisk) och väsentliga prestanda för elektriska utrustningar och system för medicinskt bruk. Den anger allmänna fordringar och detaljerade krav för flertalet utrustningstyper i form av ett antal tilläggsstandarder för bl. a. radiologisk utrustning och elektromagnetisk kompatibilitet.

28.2.7 Personuppgiftslagen (SFS 1998:204)

Personuppgiftslagens (PUL) syfte är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Denna lag gäller för sådan behandling av personuppgifter som helt eller delvis är automatiserad. Lagen gäller även för annan behandling av personuppgifter, om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Personuppgifter får behandlas bara om den registrerade har lämnat sitt samtycke till behandlingen.

Den personuppgiftsansvarige skall se till att:

1. Personuppgifter behandlas bara om det är lagligt,
2. Personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed,
3. Personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål,
4. Personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in,
5. De personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen,
6. Inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,
7. De personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella,
8. Alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen, och
9. Personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Personuppgifter får behandlas bara om den registrerade har lämnat sitt samtycke till behandlingen eller om behandlingen är nödvändig för att;

1. Ett avtal med den registrerade skall kunna fullgöras eller åtgärder som den registrerade begärt skall kunna vidtas innan ett avtal träffas,
2. Den personuppgiftsansvarige skall kunna fullgöra en rättslig skyldighet,
3. Vitala intressen för den registrerade skall kunna skyddas,
4. En arbetsuppgift av allmänt intresse skall kunna utföras,
5. Den personuppgiftsansvarige eller en tredje man till vilken personuppgifter lämnas ut skall kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller

6. Ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifterna lämnas ut skall kunna tillgodoses, om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.

Känsliga personuppgifter får behandlas för hälso- och sjukvårdsändamål, om behandlingen är nödvändig för:

1. Förebyggande hälso- och sjukvård,
2. Medicinska diagnoser,
3. Vård eller behandling, eller
4. Administration av hälso- och sjukvård.

Den som är yrkesmässigt verksam inom hälso- och sjukvårdsområdet och har tystnadsplikt får även behandla känsliga personuppgifter som omfattas av tystnadsplikten. Detsamma gäller den som är underkastad en liknande tystnadsplikt och som har fått känsliga personuppgifter från verksamhet inom hälso- och sjukvårdsområdet.

Den personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av:

1. De tekniska möjligheter som finns,
2. Vad det skulle kosta att genomföra åtgärderna,
3. De särskilda risker som finns med behandlingen av personuppgifterna, och
4. Hur känsliga de behandlade personuppgifterna är.

28.2.8 Patientdatalagen (SFS 2008:355)

Patientdatalagen (PDL) tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården. I lagen finns också bestämmelser om skyldighet att föra patientjournal.

PDL ställer kravet att vårdgivare i sina journalsystem ska kunna hantera patienters önskemål om spärr av personuppgifter. Vårdgivaren ska även kunna redovisa loggar över vilken vårdpersonal som haft åtkomst till patientens data.

Lagen syftar till att informationshantering inom hälso- och sjukvården är organiserad så att den tillgodoser patientsäkerhet och god kvalitet samt främjar kostnadseffektivitet. Personuppgifter ska utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras. Dokumenterade personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem.

Skyldig att föra en patientjournal är:

1. Den som enligt 4 kap. Patientsäkerhetslagen (SFS 2010:659) har legitimation eller särskilt förordnande att utöva visst yrke,
2. Den som, utan att ha legitimation för yrket, utför arbetsuppgifter som annars bara ska utföras av logoped, psykolog eller psykoterapeut inom den allmänna hälso- och sjukvården eller utför sådana arbetsuppgifter inom den enskilda hälso- och sjukvården som biträde åt legitimerad yrkesutövare, och

3. Den som är verksam som kurator i den allmänna hälso- och sjukvården. Lag om ändring i Patientdatalagen (SFS 2010:677).

En patientjournal ska innehålla de uppgifter som behövs för en god och säker vård av patienten.

En journalhandling ska bevaras minst tio år efter det att den sista uppgiften fördes in i handlingen. På ansökan av patienten eller någon annan som omnämns i en patientjournal får Inspektionen för vård och omsorg besluta att journalen helt eller delvis ska förstöras. Förutsättningarna för detta är att:

1. Godtagbara skäl anförs för ansökan, och
2. Patientjournalen eller den del av den som ansökan avser uppenbarligen inte behövs för patientens vård.

28.2.9 Socialstyrelsens föreskrift om informationshantering och journalföring i hälso- & sjukvården (SOSFS 2008:14)

Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- & sjukvård anger att föreskriften ska tillämpas vid vårdgivares behandling av patientens personuppgifter (patientuppgifter) vid journalföring.

Rutiner för journalföring handlar om att:

- Vårdgivaren ska säkerställa att det finns rutiner för hur patientuppgifter ska dokumenteras i patientjournaler.
- Dokumentation av patientuppgifter ska säkerställa att uppgifterna så långt möjligt dokumenteras med hjälp av nationellt fastställda begrepp och termer, klassifikationer och övriga kodverk.
- Dokumentation av patientuppgifter ska även säkerställa att patientjournalen kan utgöra ett underlag för uppföljning av vårdens resultat och kvalitet.
- Dokumentationen förses med en entydig personidentifikation.
- En patients senast kända adress eller andra kontaktuppgifter finns angivna.
- Namnet på den person som svarar för en viss journaluppgift samt även dennes befattning finns angiven.
- Tidpunkten för varje vårdkontakt som en patient ska ha eller har haft finns angiven.

Rutinerna för dokumentation av patientuppgifter ska även säkerställa att det är möjligt att föra patientjournal även när:

1. En patients identitet inte kan fastställas,
2. En patient saknar svenskt personnummer, eller
3. En patient har skyddade personuppgifter.

Rutinerna för dokumentation av patientuppgifter ska säkerställa att en patientjournal innehåller:

1. Uppgifter om aktuellt hälsotillstånd och medicinska bedömningar,
2. Uppgifter om ordinationer av t.ex. läkemedel och olika behandlingar,
3. Uppgifter om förskrivningsorsak vid ordination av läkemedel,
4. Undersökningsresultat,

5. Uppgifter om överkänslighet för läkemedel eller vissa ämnen,
6. Uppgifter om vårdhygienisk smitta, samt
7. Epikris och andra sammanfattningar av genomförd vård.

28.3 Bilaga 3 - Utredning om rätt information i vård och omsorg (SOU 2014:23)

Nedan sammanfattar vi Socialdepartementets utredning om rätt information i vård och omsorg (SOU 2014:23), ”*Rätt information i rätt tid för rätt användare*”:

Utredningen om rätt information i vård och omsorg (SOU 2014:23) föreslår en ny Hälso- och sjukvårdsdatalag och en ny Socialtjänstdatalag vilka bör träda i kraft den 1 januari 2016. När Hälso- och sjukvårdsdatalagen träder i kraft ska Patientdatalagen (SFS 2008:355) upphöra att gälla. Följdändringar måste göras i flera andra lagar. Noterbart är att Lagen om medicintekniska produkter (SFS 1993:584) inte är med bland de lagar som räknas upp.

Utredningen konstaterar att den information som behövs för att en individ ska få en god vård och omsorg inte alltid finns tillhands. Uppdraget har varit att identifiera nödvändiga förutsättningar för en ändamålsenlig och mer sammanhållen informationshantering inom och mellan hälso- och sjukvården och socialtjänsten. Den uttalade målsättningen har varit att skapa förutsättningar för en informationshantering som bidrar till ännu bättre resultat för individer som är i behov av hälso- och sjukvård. ***Rätt information i rätt tid för rätt användare*** är en nyckel till vårdpersonalens möjligheter att göra ett bra arbete för den enskilde. Uppenbart är att informationshanteringen bör vara anpassad till det konkreta arbetet i vården.

Detta förutsätter att både dokumenterandet och utbytet av information mellan de som arbetar i verksamheten fungerar på ett *ändamålsenligt* sätt. Enligt utredningens uppfattning har vi gått från en tid när det många gånger har handlat om *att* dokumentera uppgifter om enskilda, till en tid när det i större utsträckning även handlar om *hur* uppgifter som har dokumenterats kan användas för att skapa bästa möjliga resultat för individen. Utredarna pekar på att det inte råder någon tvekan om att komplexiteten i hälso- och sjukvården ökar, bland annat i takt med nya medicinska landvinningar och utvecklingen av nya läkemedel samt inte minst medicintekniska produkter. Samtidigt är nya möjligheter ofta förknippande med nya risker, exempelvis i form av otillräckligt skydd för den personliga integriteten. Det behöver därför göras en ständig avvägning mellan informationshanteringens nytta och risk.

Att begränsa patientens rätt att spärra uppgifter är rättsligt komplicerat. Det kan finnas skäl att överväga om viss information alltid behövs, som en nödvändig förutsättning, för att ge patienten en god och säker vård. Vid analysen av nyttan med tillgång till informationen relaterat till risken för ökat integritetsintrång måste särskild hänsyn tas till att läkemedel är en informationsmängd som är särskilt viktig för patientens liv och hälsa. Uppgifter om ordinerade läkemedel är ofta alldeles avgörande i vårdögonblicket. Utredningen föreslår att patienten inte har rätt att spärra uppgifter om ordinerade läkemedel, ordinationsorsak, läkemedlets namn, form, mängd, dosering, administrationssätt och tidpunkter för administrering.

Patientdatalagen har inga uttryckliga krav på vårdgivarna att se till att vårddokumentationen är tillgänglig och användbar eller att informationssystemen som används i verksamheten ska vara ändamålsenliga. Utredningen bedömer att integritetsskyddet behöver anpassas för att på bästa sätt skydda patientens integritet och möjliggöra god vård och omsorg.

Några faktorer som SOU 2014:23 pekar på:

- Behovet av att införa ett nationellt fackspråk och en informationsstruktur som stödjer ett evidensbaserat arbete.
- Behovet av att reducera de negativa konsekvenserna av regelverksorganisatoriskt fokus.
- Behovet av att de rättsliga förutsättningarna för samverkan kring enskilda patienter ligger i linje med de behov som finns för patienten.

Några av huvudpunkterna i förslaget till den nya Hälso- och sjukvårdsdatalagen är:

- Lagen syftar till att främja en informationshantering som tillgodoser god kvalitet, patientsäkerhet och kostnadseffektivitet.
- Vårdgivare ska se till att dokumenterade personuppgifter hanteras och förvaras så att obehöriga inte får tillgång till dem.
- Vårdgivare ska se till att de informationssystem som innehåller personuppgifter är lätta att använda, stödjer det kliniska arbetet, underlättar arbetet med kvalitetsutveckling, underlättar samverkan och utbyte av uppgifter mellan olika vårdgivare samt är utformade på sådant sätt att patienternas integritetsskydd tillgodoses.

Några av lagförslagets konsekvenser är:

- Enklare regler där patientens samtycke till vård också omfattar den informationshantering som krävs.
- Informationshanteringen ska bli mindre beroende av hur vård och omsorg är organiserade och istället utgå från individen och individens behov.
- De som arbetar tillsammans över organisatoriska och professionella gränser får rättsliga möjligheter att skapa en gemensam bild av individens behov och hälsosituation. Informationsutbytet kan ske genom direktåtkomst eller i en gemensam vård- och omsorgsjournal.
- Reglerna om sammanhållen journalföring i patientdatalagen har inneburit tillämpningsproblem. Utredningen ger förslag på mer ändamålsenliga rutiner i samband med vården av en patient. Tillämpningsområdet för sammanhållen journalföring minskar jämfört med vad som är fallet idag.
- För den enskilde yrkesutövaren ska det endast vara tillåtet att ta del av uppgifter om han eller hon behöver uppgifterna för sitt arbete och om uppgifterna ska användas för något av de ändamål som är tillåtna enligt lagen.
- Behörigheten ska anpassas och begränsas till vad som behövs. Vårdgivare ska göra aktiva och individuella behörighetstilldelningar och för sammanhållen journalföring skall bedömningen vila på en riskanalys.
- Konsekvenserna av utformningen av behörigheten måste beaktas både ur patientsäkerhetsaspekter och ur aspekten att skydda patientens integritet.

28.4 Bilaga 4 - Ordlista

I rapporten används begrepp och termer enligt följande definitioner:

Begrepp / Term	Förklaring	Källa
Aktivt val	Funktion i verksamhetssystem som innebär att användaren breddar sin möjlighet att ta del av uppgifter om en patient som finns registrerad hos andra vårdenheter hos samma vårdgivare.	Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14)
Behandling av personuppgifter	Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.	Personuppgiftslagen (1998:204)
Behörighet	En användares faktiska möjlighet att ta del av uppgifter, exempelvis i ett av hälso- och sjukvårdens journalsystem.	Utredningen om rätt information i vård och omsorg (SOU 2014:23)
Behörighetsstyrning	Organisatoriska, administrativa och tekniska åtgärder som vidtas för att anpassa och begränsa behörigheten till patientuppgifter efter användarens behov för att denne skall kunna utföra sitt arbete.	Utredningen om rätt information i vård och omsorg (SOU 2014:23)
Epikris	Sammanfattande bedömning i en patientjournal.	Nationalencyklopedin
Huvudman	Den som enligt hälso- och sjukvårdslagen (SFS 1982:763) ansvarar för att erbjuda hälso- och sjukvård. Inom en huvudmans geografiska område kan en eller flera vårdgivare bedriva verksamhet.	Utredningen om rätt information i vård och omsorg (SOU 2014:23)
Hybridintegration	Hybrid betyder "blandning" och integration betyder ”förening”. Hybridintegration är en eller flera olika tekniker, Uthoppsintegration Överföringsintegration etc., i kombination	Begrepp definierat av arbetsgruppen.

Begrepp / Term	Förklaring	Källa
	för att koppla samman flera olika fristående system för att dela information.	
Informationssystem	System som samlar in, bearbetar, lagrar eller distribuerar och presenterar information.	Användning av medicintekniska produkter i hälso- och sjukvården (SOSFS 2008:1)
Insynsskydd och kryptering	Teknisk mekanism för att förhindra obehörig åtkomst till information.	Allmänt vedertaget enligt Arbetsgruppen
IVO	Inspektionen för vård och omsorg.	http://www.ivo.se
Journalföring	Vid vård av patienter ska det föras patientjournal. En patientjournal ska föras för varje patient och får inte vara gemensam för flera patienter.	Patientdatalagen (SFS 2008:355)
Journalhandling	Framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel och som upprättas eller inkommer i samband med vården av en patient och som innehåller uppgifter om patientens hälsotillstånd eller andra personliga förhållanden eller om vidtagna eller planerade vårdåtgärder.	Patientdatalagen (SFS 2008:355)
Journaluppgift	All slags information som är noterad i en patientjournal och som direkt eller indirekt kan hänföras till en fysisk person.	Kombination av Personuppgiftslagen (SFS 1998:204) och Patientdatalagen (SFS 2008:355)
Lagen om medicintekniska produkter (LMP)	Lag om allmänna bestämmelser om medicintekniska produkter.	Lagen om medicintekniska produkter (SFS 1993:584)
Medicinteknisk produkt (MTP)	Med en medicinteknisk produkt avses en produkt som enligt tillverkarens uppgift ska användas, separat eller i kombination med annat, för att hos människor: 1. Påvisa, förebygga, övervaka, behandla eller lindra en sjukdom.	Lagen om medicintekniska produkter (SFS 1993:584)

Begrepp / Term	Förklaring	Källa
	2. Påvisa, övervaka, behandla, lindra eller kompensera en skada eller en funktionsnedsättning. 3. Undersöka, ändra eller ersätta anatomin eller en fysiologisk process. 4. Kontrollera befruktning.	
Medicinteknisk utrustning (MTU)	Ingår som en delmängd i begreppet ”Medicinteknisk produkt”.	http://www.socialstyrelsen.se/patientsakerhet/riskomraden/medicinteknik
Medicintekniskt system	Ingår som en delmängd i begreppet ”Medicinteknisk produkt” och består av två eller flertal tekniska produkter, med eller utan IT-produkter, som samverkar i ett system för medicinsk avsedd användning	Begrepp definierat av arbetsgruppen.
mHälsa	Begreppet mHälsa baseras på Världshälsoorganisationens (WHO) definition av begreppet hälsa, vilket beskrivs som ”Ett tillstånd av fullständigt fysiskt, psykiskt och socialt välbefinnande”. Genom att addera ”m” till hälsobegreppet signaleras möjligheten att uppnå dessa nyttoeffekter för individen genom en bred användning av mobil informations- och	Läkemedelsverket
MIS	Medicinska informationssystem	Läkemedelsverket
MT-data	Tekniskt genererad (insamlad/bearbetad) information från medicinteknisk produkt, av patients biologiska mätdata (person-uppgifter i form av mätdata) som ännu ej bedömts av legitimerad vårdpersonal vara autentisk och väsentlig för patientens diagnostik eller vård och därmed föremål att journalföras i patientens ordinära journal. *(När MT-data journalförs blir den en journaluppgift/undersökningsresultat)*	Nytt begrepp definierat av arbetsgruppen.
Ordinära journalföringen	Den patientjournal som man i första hand vänder sig till när man söker en journalhandling.	Patientdata och läkemedel m.m. (SOU 2007:48)

Begrepp / Term	Förklaring	Källa
Patientdatalagen (PDL)	Denna lag tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården.	Patientdatalagen (SFS 2008:355)
Patientjournal	En eller flera journalhandlingar som rör samma patient.	Patientdatalagen (SFS 2008:355)
Patientdata	Se Patientuppgift	Datainspektionen
Patientuppgift	Patientens personuppgifter *(Är en synonym av termen **journaluppgift**)*	Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14)
PDL-loggning	Åtkomstlogg till enskild patients journaluppgifter. Ska vara utformad så att patienten kan uttyda om åtkomsten varit befogad eller ej.	Patientdatalagen (SFS 2008:355)
Personuppgift	Information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.	Personuppgiftslagen (SFS 1998:204)
Personuppgifts-ombud	En person - ofta en anställd - som ser till att personuppgifter behandlas korrekt och lagligt inom en verksamhet.	Datainspektionen
Personuppgiftslagen (PUL)	Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.	Personuppgiftslagen (SFS 1998:204)
Primärjournal	Se "Ordinära journalföringen".	Patientdata och läkemedel m.m. (SOU 2007:048)
Rådata	Obearbetade data.	Bonniers svenska ordbok, 10:e upplagan
Sammanhållen journalföring	Ett elektroniskt system, som gör det möjligt för en vårdgivare att ge eller få direktåtkomst till personuppgifter hos en annan vårdgivare.	Patientdatalagen (SFS 2008:355)
Samtycke	Med samtycke menas varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken den som registreras, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne.	www.datainspektionen.se/ ordlista

Begrepp / Term	Förklaring	Källa
Sekundärjournal	Personuppgifter som behandlas separat från den ordinära journalföringen (t.ex. vid medicinska serviceenheter).	Patientdata och läkemedel m.m. (SOU 2007:48)
SI-nätverket	Nationellt nätverk bestående av personer som arbetar med frågor inom området Medicinsk Teknik och IT. Detta nätverk har till syfte att knyta samman gemensamma intressen runt om i Sverige inom detta område.	http://www.lfmt.se/si-forum.html
SITHS-kort	Tjänstelegitimation för både fysisk och elektronisk identifiering. Ett ordinarie SITHS-kort innehåller ett personligt e-leg som visar vem du är, och ett SITHS-certifikat som visar identiteten i din yrkesroll. (Uppfyller kraven på stark autentisering).	http://www.inera.se/tjanster--projekt/siths
Spärr (patientens begärda spärrar)	***Inre spärr*** De personuppgifter som dokumenterats för ändamålet som anges i PDL 2 kap. 4 § första stycket 1 och 2 hos en vårdenhet eller inom en vårdprocess får inte göras tillgängliga genom elektronisk åtkomst för den som arbetar vid en annan vårdenhet eller inom en annan vårdprocess hos samma vårdgivare, om patienten motsätter sig det. ***Yttre spärr*** De personuppgifter som dokumenterats för ändamålet som anges i PDL 2 kap. 4 § första stycket 1 och 2 hos en vårdgivare får inte göras tillgängliga genom elektronisk åtkomst (sammanhållen journalföring) för den som arbetar vid en annan vårdgivare, om patienten motsätter sig det.	Patientdatalagen (SFS 2008:355)
Stark autentisering	Autentisering som innebär att identiteten kontrolleras på två olika sätt.	Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14)
Vårddokumentation	Personuppgifter som behandlas inom hälso- och sjukvården om det behövs för:	Utredningen om rätt information i vård och omsorg (SOU 2014:23)

Begrepp / Term	Förklaring	Källa
	1. Att förebygga, utreda eller behandla sjukdomar och skador hos patienter. 2. Att upprätta annan dokumentation som behövs i och för vården av patienter. 3. Administration som rör patienter och som syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall. 4. Att upprätta annan dokumentation som följer av lag, förordning eller annan författning. 5. Att systematiskt och fortlöpande utveckla och säkra kvaliteten i verksamheten. 6. Administration, planering, uppföljning, utvärdering och tillsyn av verksamheten. 7. Att framställa statistik om hälso- och sjukvården.	
Vårdenhet	Organisatorisk enhet som tillhandahåller hälso- och sjukvård vars omfattning vårdgivaren själv fastställer. Ofta den verksamhet som leds av en verksamhetschef.	Utredningen om rätt information i vård och omsorg (SOU 2014:23)
Vårdgivare	Statlig myndighet, landsting och kommun i fråga om sådan hälso- och sjukvårdsverksamhet som myndigheten, landstinget eller kommunen har ansvar för (offentlig vårdgivare) samt annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvårdsverksamhet (inkl. privat vårdgivare).	Patientdatalagen (SFS 2008:355)