Ledningsnätverket för Medicinsk Teknik

Utredning

Patientdatalagen i den kliniska vardagen

- Vilka krav ställs på medicintekniska produkter

Rapport Del 2:

Tillämpning av informationssäkerhet i medicintekniska produkter

2016-09-30

Sammanfattning

Ledningsnätverket för Medicinsk Teknik (LfMT) är sjukvårdshuvudmännens gemensamma forum inom det medicintekniska (MT) området (www.lfmt.se). I syfte att utreda och föreslå hur konflikten mellan de icke harmoniserande regelverken Patientdatalagen (PDL) och Lagen om medicintekniska produkter (LMP) kan hanteras, tillsatte LfMT under 2014 en arbetsgrupp bestående av medlemmar från SI-nätverket inom LfMT. Resultatet presenterades 2015 i rapporten ”*Patientdatalagen i den kliniska vardagen - Vilka krav ställs på medicintekniska produkter*” (i fortsättningen benämnd ”Del 1”). Denna rapport fick god spridning och slutsatserna blev väl mottagna bland majoriteten av aktörerna inom hälso- och sjukvård i Sverige. Datainspektionen var i princip ensam om en klart avvikande uppfattning.

Denna uppföljande rapport (”Del 2”) består av två huvudavsnitt:

I) Redovisar responsen som gavs på Del 1. Den generella uppfattningen i responsen på Del 1 är att det är viktigt att man balanserar kraven på åtgärder för skydd av individens integritet med kraven på väsentligt skydd för liv och hälsa. Det saknas dessvärre riktlinjer från myndigheterna om hur man praktiskt ska förfara för att uppnå en god balans mellan dessa båda skyddsvärden. Beskeden som LfMT hittills har fått vid dialog med olika myndigheter och andra aktörer är att man ska säkerställa dem båda så långt som det låter sig göras.

II) Behandlar det huvudsakliga syftet med denna rapport; Att testa och visa hur informationsbegreppet *MT-data,* vilket definierades i Del 1, kan användas för att överbrygga de icke harmoniserande regelverken Patientdatalagen (PDL) och Lagen om medicintekniska produkter (LMP). Avsnitt II redovisar resultatet av en litteraturstudie. Här finns också förslag på konkreta riktlinjer och rekommendationer till aktörerna inom MT-området, bl a via en omarbetning och utvidgning av checklistan från Del 1.

I syfte att konkretisera och exemplifiera tillämpningen av begreppet *MT-data,* så redovisas ett fiktivt patientfall där läsaren får följa en hjärtpatients väg genom ett förenklat vårdprogram. Det finns i huvudsak fyra lagar som berör informationshanteringen inom offentlig hälso- och sjukvård. Med dessa som utgångspunkt så kompletteras exemplet med hur *MT-data* bör hanteras i dess väg till att bli ett undersökningsresultat i patientens journal.

LfMT:s grundläggande uppfattning bygger på att nyttan med medicintekniska produkter (MTP) vida ska överstiga den risk som patienten utsätts för. LfMT föreslår i rapporten en modell som utgår från tidskriterier för balansering mellan skydd av liv och hälsa och skydd av patientens integritet. Tidskriterierna bör användas som riktlinje för hur lång tid det maximalt får ta att åtgärda eventuella hinder för åtkomst till *MT-data*. Hur detta kan gå till beskrivs i exempel.

Rapporten avslutas med LfMT:s rekommendationer avseende de problemställningar som behandlas, samt ger förslag på fortsatt arbete inom området. LfMT konkretiserar också vilka specifika krav tillverkare och vårdgivare bör hantera var för sig och vilka som bör hanteras tillsammans. LfMT rekommenderar myndigheterna SoS, IVO och LV att ge ut tydliga instruktioner till alla aktörer om hur man ska hantera och betrakta *MT-data* under dess väg från patient till journalhandling.

Sjukvården hanterar dagligen mycket stora volymer *MT-data*. I väntan på att PDL revideras så rekommenderar LfMT att man använder PUL som stöd avseende hur *MT-data* ska behandlas. Denna rekommendation tycker många av vårdens aktörer och ett antal av de jurister vi varit i kontakt med är intressant och som de anser att LfMT bör vidareutveckla. Denna rapport är en vidareutveckling av detta synsätt. Den är också avsedd att vara ett stöd att i den kliniska miljön hantera information, från MTP och vilken vi benämner som *MT-data,* enligt PUL och PDL:s intentioner.

Innehållsförteckning

Inledning

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).

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.

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 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.

Utredningsrapporten från detta arbete; ”*Patientdatalagen i den kliniska vardagen - Vilka krav ställs på medicintekniska produkter*” (i fortsättningen benämnd ”Del 1”), publicerades i samband med ett heldagsseminarium 2015-03-25 och kan nu anses som väl spridd bland de olika aktörerna verksamma inom hälso- och sjukvård i Sverige. Detta gäller såväl landsting/regioner, leverantörer och myndigheter som verkar inom kompetensområdet medicinteknisk IT, samt juridiska företrädare inom området informationssäkerhet.

LfMT:s konklusion av reaktionerna på Del 1 är att rapporten allmänt anses som viktig och att den publicerades vid rätt tidpunkt. Arbetsgruppen har efter publiceringen presenterat rapporten i olika sammanhang och mottagit många kloka synpunkter, reflektioner och förslag på förtydliganden av innehållet samt uppmuntran att fortsätta arbetet. LfMT har därför beslutat ge arbetsgruppen i uppdrag att värdera och konkretisera dessa, vilket resulterat i denna rapport; ”*Patientdatalagen i den kliniska vardagen - Del 2: Tillämpning av informationssäkerhet i medicintekniska produkter*”.

Utgångspunkten för denna rapport är det informationsbegrepp, ”*MT-data*”, som vi definierade i Del 1:

> *Tekniskt genererad (insamlad och/eller 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”*.

Under arbetets gång med Del 2 så har vi insett att definitionen, i vår ansats att den skall vara entydig, kan uppfattas som omständlig och abstrakt. För ”vardagsbruk” anser LfMT därför att definitionen kan sammanfattas som att:

> *”MT-data” är ännu ej journalförd information från MTP.*
> *Journalförd ”MT-data” benämns som ”undersökningsresultat”.*

Ett huvudsakligt syfte med denna Del 2 är att gå vidare med ansatsen från Del 1 och testa och visa hur informationsbegreppet *MT-data* kan användas för att överbrygga problemen med att Patientdatalagen (PDL) inte harmoniserar med Lagen om medicintekniska produkter (LMP) och Patientsäkerhetslagen (PSL).

Uppdragsägare och arbetsgrupp

Uppdragsgivare, uppdragsägare och utgivare av rapporten:
LfMT via styrelsen LfMT

Arbetsgrupp:
Kjell Andersson, Västra Götalandsregionen, Uppdragsledare och ordförande i SI-nätverket
Hans-Olof Carlsén, Region Örebro Län
Jan-Olof Dahlberg, Västerbottens läns landsting
Stig Wiinberg, Region Skåne

Termer och begrepp

Tabellen nedan definierar ett antal termer och begrepp som används i rapporten:

Begrepp / Term	Förklaring	Källa
Allmän handling	Varje handling som har kommit in till eller är upprättad hos en statlig eller kommunal myndighet och som förvaras hos myndigheten. Handlingen kan vara i pappersform, innehållet i ett e-brev, ett ljud- eller videoband, en CD eller en diskett, och så vidare. Offentlighetsprincipen innebär att vem som helst får begära ut en allmän handling. Myndigheten ska då göra en sekretess-prövning och handlingen ska lämnas ut om inte sekretess föreligger. Jfr *Upprättad handling* nedan.	www.datainspektionen.se/ ordlista
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.	Personuppgiftslag (1998:204, 3 §)
Behörighet	En individs 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)

Begrepp / Term	**Förklaring**	**Källa**
Hybridintegration	*Hybrid* betyder "blandning" och *integration* betyder ”förening”. Hybridintegration är en eller flera olika tekniker i kombination för att koppla samman flera olika fristående system för att dela information, t. ex. Uthoppsintegration och Överförings-integration.	Begrepp definierat av arbetsgruppen.
Informationssystem	System som samlar in, bearbetar, lagrar eller distribuerar och presenterar information.	Användning av medicintekniska produkter i hälso- och sjukvården (SOSFS 2008:1, 2 kap. 1 §)
IVO	Inspektionen för vård och omsorg.	http://www.ivo.se
Journal	Vid vård av patienter ska det föras patientjournal. En patientjournal ska föras för varje patient och får inte vara gemensam för flera patienter. En patientjournal ska innehålla de 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 bakgrunden till vården, 3. uppgift om ställd diagnos och anledning till mera betydande åtgärder, 4. väsentliga uppgifter om vidtagna och planerade åtgärder, och 5. uppgift om den information som lämnats till patienten och om de ställningstaganden som gjorts i fråga om val av behandlingsalternativ och om 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.	Patientdatalag (SFS 2008:355, 3 kap. 1 § och 6§)
Journalhandling	Handlingar som upprättas av den som är skyldig att föra journal vid vård av patienter eller inkommer i samband med vården och som rör patientens hälsotillstånd eller andra personliga förhållanden. Framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med	http://www.socialstyrelsen.se/fragorochsvar/patientjournaler Patientdatalag (SFS 2008:355, 1 kap. 3 §)

Begrepp / Term	**Förklaring**	**Källa**
	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.	
Journaluppgift	All slags information som är noterad i en patientjournal och som direkt eller indirekt kan hänföras till en fysisk person.	Patientdatalag (SFS 2008:355, 3 kap.)
Lagen om medicintekniska produkter (LMP)	Lag om allmänna bestämmelser om medicintekniska produkter.	Lag 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. 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.	Lag om medicintekniska produkter (SFS 1993:584, 2 §)
MT-system	*Medicintekniska system* ingår som en delmängd i begreppet *Medicinteknisk produkt* och består av hela eller delar av två eller flera produkter, med eller utan IT-anknytning, vilka samverkar i ett system som av tillverkaren är avsett för medicinsk användning.	Läkemedelsverket (LVFS 2003:11, 2 §)
mHälsa	Mobil hälsoprodukt. Mobil hälsa omfattar praxis inom medicinsk och folkhälsa vilka stöds av mobila enheter, som smarta telefoner, patientövervakningsanordningar, personliga digitala assistenter och andra trådlösa enheter. Den innehåller också applikationer (”appar”) såsom livsstils- och välbefinnandeprogram som kan ansluta till medicintekniska produkter eller sensorer (t. ex. armband eller klockor) samt personliga styrsystem för hälsoinformation och påminnelser om medicinering.	Läkemedelsverkets seminarium om medicintekniska produkter och mHälsa
MIS	Medicinska informationssystem.	Läkemedelsverket

Begrepp / Term	**Förklaring**	**Källa**
MT-data	MT-data är ännu ej journalförd information från MTP: Tekniskt genererad (insamlad och/eller 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". *(När MT-data journalförs blir den en journaluppgift/ett undersökningsresultat)*	Nytt begrepp definierat av arbetsgruppen.
Patientdata	Se "Patientuppgift".	--
Patientdatalagen (PDL)	Lag som reglerar vårdgivares behandling av personuppgifter inom hälso- och sjukvården.	Patientdatalag (SFS 2008:355)
Patientjournal	En eller flera journalhandlingar som rör samma patient.	Patientdatalag (SFS 2008:355)
Patientsäkerhets-lagen (PSL)	Patientsäkerhetslagen syftar till att främja hög patientsäkerhet inom hälso- och sjukvård och därmed jämförlig verksamhet. I lagen finns bestämmelser bland annat om; - vårdgivarens skyldighet att bedriva ett systematiskt patientsäkerhetsarbete (3 kap.), - behörighetsfrågor (4 kap.), - skyldigheter för hälso- och sjukvårdspersonal m.fl. (6 kap.), - Inspektionen för vård och omsorgs tillsyn (7 kap.)	Patientsäkerhetslagen (SFS 2010:659)
Patientuppgift	Patientens personuppgifter i journalen. *(Är en synonym av termen "Journaluppgift")*	Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14)
Personuppgift	All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. All slags information som direkt eller indirekt kan knytas till en (fysisk) person som är i livet. Även bild- och ljuduppgifter om en (fysisk) person räknas som personuppgifter, även om inga namn nämns. Krypterade eller kodade uppgifter	Personuppgiftslag (SFS 1998:204, 3 §) www.datainspektionen.se/ordlista

Begrepp / Term	Förklaring	Källa
	är också personuppgifter om någon har en nyckel som kan koppla dem till en person.	
Personuppgifts-ombud	Den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt skall se till att personuppgifter behandlas på ett korrekt och lagligt sätt.	Personuppgiftslag (SFS 1998:204, 3 §)
Personuppgiftslagen (PUL)	Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.	Personuppgiftslag (SFS 1998:204, 1 §)
Sammanhållen journalföring	Direktåtkomst till uppgifter hos en annan vårdgivare. Ett elektroniskt system, som gör det möjligt för en vårdgivare att ge eller få direktåtkomst till personuppgifter hos en annan vårdgivare.	Patientdatalag (SFS 2008:355, 6 kap.)
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
Samverkansgruppen för informations-säkerhet (SAMFI)	Myndigheterna i SAMFI stödjer varandra i arbetet med samhällets informationssäkerhet genom informationsutbyte och samverkan. Följande myndigheter ingår i SAMFI: - Myndigheten för samhällsskydd och beredskap (MSB) - Post- och telestyrelsen (PTS) - Polismyndigheten - Försvarets radioanstalt (FRA) - Säkerhetspolisen (Säpo) - Försvarets materielverk (FMV)/Sveriges Certifieringsorgan för IT-säkerhet (CSEC) - Försvarsmakten (FM)/Militära underrättelse- och säkerhetstjänsten (MUST)	https://www.informationssakerhet.se
SI-nätverket	Nationellt nätverk inom LfMT 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	SITHS står för *Säker IT för Hälso- och sjukvården*. Tjänstelegitimation för både fysisk och elektronisk identifiering. Ett	http://www.inera.se/tjanster--projekt/siths

Begrepp / Term	Förklaring	Källa
	ordinarie SITHS-kort innehåller en personlig e-legitimation som visar vem du är, och ett SITHS-certifikat som visar identiteten i din yrkesroll. (SITHS Uppfyller kraven på stark autentisering).	
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 hos en annan vårdgivare, om patienten motsätter sig det.	Patientdatalag (SFS 2008:355, 4 kap. 4 § samt 6 kap. 2 §)
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)
Upprättad handling	Enligt Tryckfrihetsförordningen ska en handling anses upprättad: - när den har expedierats - när det ärende, till vilket den hör, har slutbehandlats; eller - när den på annat sätt färdigställts. Handlingar som inte expedieras och inte tillhör ärenden, t. ex. fristående skrivelser och utredningar, blir alltså allmänna när de är färdigställda. Protokoll blir enligt samma paragraf allmänna efter justering. Vad gäller diarier, register, journaler så räknas de som upprättade så snart de är färdiga att tas i bruk. Man behöver alltså inte ha börjat föra in uppgifter i dem. Händelser av vikt i ett ärende som lämnats muntligt t.ex. vid ett telefonsamtal eller annan muntlig kontakt eller som inkommer skriftligt via t ex SMS ska dokumenteras. Denna s.k. tjänsteanteckning är en upprättad allmän handling.	Tryckfrihetsförordning (SFS 1949:105, 2 kap. 7 §) www.samradsgruppen.se/web/index.php/offentlighetslagstiftningen/offentlighetsprincipen-och-hantering-av-allmaenna-handlingar

Begrepp / Term	**Förklaring**	**Källa**
	Jfr *Allmän handling* ovan.	
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 (privat vårdgivare).	Patientdatalag (SFS 2008:355, 1 kap. 3 §)

Avsnitt I:

Respons på den ursprungliga utredningsrapporten (*Del 1*)

Aktiviteter, möten och respons

Seminariedag

Del 1 presenterades onsdagen den 25 mars 2015 i SKL-huset i Stockholm i form av en seminariedag med rubriken:

Patientdatalagen i den kliniska vardagen - Vilka krav ställs på medicintekniska produkter?

Målen med seminariedagen var att:

- Presentera utredningsrapporten.
- Bringa klarhet i den aktuella situationen.
- Åstadkomma en nationell samsyn och ge signaler till berörda myndigheter inför beredning av eventuella förändringar i regelverket.
- Ge vägledning till de som är verksamma i den kliniska vardagen.
- Initiera en fortsatt diskussion om informationssäkerhet i medicintekniska produkter.

Program:

- **Presentation av LfMT:s utredning: Patientdatalagen i den kliniska vardagen - Vilka krav ställs på medicintekniska produkter?**
  Jan-Olof Dahlberg, Petter Eriksson och Stig Wiinberg från SI-nätverkets arbetsgrupp

- **Informationssäkerhet i vården – Begränsningar och möjligheter**
  Michael Patriksson, Informationssäkerhetssamordnare, Landstinget Västmanland

- **Leverantörernas syn på informationssäkerhet och PDL**
  Peter Löwendahl, Swedish Medtech/Global Vice President Quality & Regulatory Affairs, Elekta AB

- **Att utveckla informationssäker MTP inom ramen för PDL**
  Ann-Sofi Mikaelsson, General Manager, Sectra Sverige AB

- **Internationell leverantör med global produktportfölj möter PDL**
  Fredrik Sandberg, Kvalitetsansvarig, Siemens Healthcare

- **Tillämpning av PDL i den praktiska vårdsituationen**
  Eva Backlund, Medicinskt ansvarig sjuksköterska, Aleris AB

- **Dataskyddsreglernas krav på informationssäkerhet i vården – Datainspektionens roll**
  Magnus Bergström, IT-säkerhetsspecialist, Datainspektionen

- **Informationssäkerhet och medicintekniska produkter**
  Mats Ohlson, Strategisk tillsynssamordnare/Senior expert medicinteknik, Läkemedelsverket

- **PDL i förändring**
  Maria Jacobsson, Regeringskansliet, Socialdepartementet, Utredningssekreterare SOU 2014:23

- **Hur skapar vi harmoniserande regelverk för informationssäkerhet respektive medicintekniska produkter?**
  Paneldiskussion med samtliga föreläsare

Möte med Socialdepartementets Samrådsgrupp för nationell eHälsa

Sjukvårdsministerns politiska sakkunnige Henrik Moberg och IngaLill Karlström, sakkunnig inom socialtjänsten, båda från Socialdepartement, bjöd in LfMT:s arbetsgrupp, representerad av Stig Wiinberg, för att vid mötet den 27 maj 2015 presentera vår rapport för Socialdepartementets samrådsgrupp för nationell eHälsa. Henrik ansåg att:

- Vår rapport är mycket intressant och kreativ.
- Vi belyser och breddar problemområdet på ett mycket bra sätt.
- Vi för fram intressanta tankegångar och perspektiv, vilka delvis kan uppfattas som helt nya.
- Rapporten uppfattas som viktig.

Samrådsgruppen består av följande aktörer (i alfabetisk ordning):
Almega (privatvården), E-hälsomyndigheten, Ersta diakoni/Stadsmissionen, Försäkringskassan, Inera, IVO, Kommunal, KTH, LIF, Läkarförbundet, Läkemedelsverket, Myndigheten för delaktighet, Privattandläkarna, Socialstyrelsen, Socialtjänsten, Swedish Medtech, Svenska sjuksköterskeförbundet, Sveriges Apoteksförening, SKL, Tandläkarförbundet, Vinnova och Vårdförbundet.

Möte med SoS och IVO

LfMT:s representanter Hans-Olof Carlsén, Kjell Andersson och Stig Wiinberg träffade den 9 juni 2015 Socialstyrelsens (SoS) jurist Cecilia Törnblom och Inspektionen för vård och omsorgs (IVO) jurist Anders Alexandersson samt IVO:s utredare/samordnare för medicinteknik, Lars Asteborg.
LfMT redovisade i korta drag innehållet i utredningsrapporten avseende problembeskrivning, utredningens resultat samt obesvarade frågeställningar att diskutera.

Representanterna från SoS och IVO hade innan mötet samrått med företrädare för Läkemedelsverket (LV) om hur man ska betrakta information från MTP. Vi tolkar deras respons på våra synpunkter avseende detta längre ner i denna rapport under rubriken: ”När blir *MT-data* en Journalhandling?”

Som representanter för brukarna av MTP fick vi följande generella uppmaningar:
- Vi ska anmäla brister i behörighetssystem och informationssäkerhet till LV och aktuell tillverkare.
- Vi bör läsa och sätta oss in i vägledningen till SOSFS 2008:14 (Föreskrifter om informationshantering och journalföring).
- Vi bör stämma av med arkiveringsfunktionen inom respektive landsting/region om hur vi får/ska gallra ut information som ej är journalhandling och som lagras i våra arkiv kopplade till MTP.
- Vi bör gärna läsa IVO:s beslut om åtgärdande av problem med Take Care vid Karolinska sjukhuset. (Se http://www.ivo.se/globalassets/dokument/bilder-och-nyheter/2015/beslut-take-care-karolinska-2015-05-18.pdf)
- Vi bör vara tydliga med bör-krav om informationssäkerhet vid upphandling av MTP.

SoS och IVO gav också följande kommentarer om vår rapport:
- Det mesta som står i vår rapport är i överensstämmelse med gällande lagstiftning och regelverk
- Vår övergång till att följa PUL i stället för PDL är intressant.
- Begreppen ordinär och sekundär journal bör vi inte använda oss av, då dessa begrepp saknar en vedertagen definition.

- Enligt SOSFS 2008:1 (Användning av MTP) så är ”Information från MTP” den korrekta benämningen på det vi i vår slutrapport benämner ”*MT-data*”.

Möte med chefjurist Sofia Melander och jurist Kim Strandberg

LfMT, representerat av Stig Wiinberg, hade den 11 juni 2015 ett möte med Chefsjurist Sofia Melander och personuppgiftsansvarige Kim Strandberg från Region Östergötland om informationssäkerhet, PDL och MTP.

Sofias uppfattning var att:

- Patienters personuppgifter i hälso- och sjukvården, så som den inledande lagtexten är formulerad, ligger inom lagrummet för PDL.
- Definitionen av begreppet journalhandling är för vid i PDL. Den borde ges en mer precis definition.
- PDL, med underliggande författningar, ger för lite information och stöd till verksamheterna om hur personuppgifter i vården, som inte är journalhandlingar, ska hanteras.
- Vår rapports beskrivning av brytpunkten, när en patientuppgift ska betraktas som journaluppgift, är bra.
- PUL har tydliga anvisningar om hur informationssäkerheten ska hanteras, så vi kommer inte undan krav på informationssäkerhet när vi tillämpar PUL istället för PDL.

Övrig respons från viktiga aktörer

Här följer en sammanställning av hur vi uppfattat den respons på Del 1 som kommit oss tillhanda från olika viktiga aktörer (i alfabetisk ordning) inom det aktuella området:

Datainspektionen:

- PDL gäller alltid när en vårdgivare behandlar personuppgifter inom hälso- och sjukvården - Oavsett *hur* eller *med vad*.
- Informationssäkerhetskraven som särregleras i PDL rör *åtkomst* till personuppgifter d v s behörighetstilldelning och åtkomstkontroll.
- Säkerhetsbestämmelserna i 2 kap. SOFS 2008:14 (Informationshantering och journalföring) är också tillämpliga.

E-Hälsomyndigheten:

- Bra presentation av situationen och problemet.
- Myndigheten kommer att jobba vidare med frågan.

Informationssäkerhetsexpert Michael Patriksson, Landstinget Västmanland:

- Bra att vi lyfter frågan och vikten av att adekvata riskanalyser avseende informationssäkerheten genomförs.
- Policy inom Landstinget Västmanland: Upphandling, utveckling och förändring av funktioner som kan påverka informationssäkerheten ska ske enligt en fastställd metod där säkerhetsaspekter har en framträdande roll.

IVO:

- Det är förhållandevis få patienter som klagar på att deras information har spritts för mycket.
- Det är däremot väldigt många patienter som klagar på att sjukvården inte använder den information som finns om dem i våra system.
- Otillgänglighet till befintlig information är idag det stora problemet inom området.

Läkemedelsverket:

- Vill veta mer om våra tankar om hur de kan hjälpa till.
- Läkemedelsverket har e-Hälsa som nytt fokusområde.
- Informerade om att Mats Ohlson (som tidigare bl. a. arbetade med dessa frågor inom LV) stödjer vårt arbete och gärna skulle se en engelskspråkig version av utredningsrapporten för spridning inom EU.

Svenska Läkaresällskapet:

- En bra och mycket viktig rapport från LfMT.
- Bra att LfMT för upp frågan på dagordningen.
- Bra att LfMT pekar på det etiska dilemmat och inte ger svar på det, utan hänvisar till att andra aktörer måste agera.

Socialstyrelsen:

- PDL och Lag om MTP måste kunna samverka.
- Skyddet av patientens integritet är mycket viktigt.
- Övertolkningar av PDL måste hanteras till en rimlig nivå.
- LfMT har en viktig roll att hjälpa till med att hitta balansen mellan de olika regelverken.

Utredningssekreterare SOU 2014:23 (*”Rätt information på rätt plats i rätt tid*”) Maria Jacobsson:

Bland utgångspunkterna för utredningen kan följande nämnas, vilka även ligger till grund för resonemangen i vår Del 1:

- Individen och individens behov i centrum
- Patientsäkerhet och god kvalitet
- Starkt integritetsskydd
- Stöd för yrkesutövare i vård och omsorg

Utredningens slutbetänkande innehåller bl. a. förslag till en ny *”Hälso- och Sjukvårdsdatalag”,* där en av de bärande tankarna är att ett välbalanserat integritetsskydd är en förutsättning för hög kvalitet och säkerhet.

I lagförslaget föreslås i 4 § att en vårdgivare ska se till att de informationssystem som innehåller personuppgifter och som används i och för vården av en patient:

- Är lätta att använda.
- Stödjer det kliniska arbetet.
- Underlättar arbetet med att utveckla kvaliteten i verksamheten.
- Underlättar samverkan och utbyte av uppgifter.
- Är utformade på ett sådant sätt att patientens integritetsskydd tillgodoses.

Lagen ska särskilt främja att:

- Den som arbetar hos en vårdgivare säkert, snabbt och enkelt får tillgång till de personuppgifter som han eller hon behöver för att kunna utföra sitt arbete
- Personuppgifter utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras.

Detta stämmer väl överens med vad vi uttrycker i Del 1.

Swedish MedTech:

- Vill gärna ha en nationell lösning på hur integritetsskyddet ska se ut för MTP.
- Ser gärna en samordning med minst ett stort EU-land, helst flera och om möjligt hela EU.
- Tillverkarna kan inte åläggas att bygga unika lösningar till vart och ett av Sveriges landsting/regioner.

- Föreslår skapande av ett nationellt tvärprofessionellt forum för samråd kring informationssäkerhetsfrågor avseende användningen av MTP, med representation från industri, sjukvård och berörda myndigheter.

Vinnova:

- Integrationsskyddet är mycket viktigt. Det måste hanteras och säkras i sjukvården också.
- LfMT får gärna ta fram förslag på innovativa tekniska lösningar för att skapa en ändamålsenlig hantering av informationsskydd i MTP.

Sammanfattning av responsen på Del 1

Problembeskrivningen i vår rapport har blivit bekräftad från en rad olika håll. Kortfattat handlar det om att regelverken PDL, LMP och PSL inte korrelerar med och inte ens hänvisar till varandra. Regelverket för MTP innehåller ringa information och vägledning om hur ett integritetsskydd ska utformas. PDL är å sin sida utformad för skydd av journalinformation, men tolkas av vissa som att den även gäller för all information genererad av MTP, oberoende av huruvida dess autenticitet bedömts och bekräftats. PSL är tydlig med att patienten har rätt till en säker hälso- och sjukvård.

Detta leder till oklara krav på traditionella implementeringar av MTP, som tillverkare har svårt att hantera. Internationella tillverkare av MTP ser uppenbara svårigheter med anpassningar av sina produkter till PDL. Det finns i vårdverksamheten stora svårigheter att hantera de ibland motstridiga kraven från PDL respektive LMP. Det finns ett stort behov av att tydliggöra var gränsen går för när information från MTP ska betraktas som en journalhandling och regleras enligt PDL. Åtgärder som stärker informationssäkerheten måste även de riskhanteras, så att de i sig inte innebär en ny fara för patientens liv och hälsa.

Problembeskrivningen kan konkretiseras till att omfatta fyra områden:

1. I vilken mån utformningen av informationssäkerheten och behörighetsskyddet inverkar negativt på effektiviteten i vårdarbetet och därmed riskerar att fysiskt skada patienten genom antingen en felaktig diagnos och behandling eller utebliven medicinsk nödvändig åtgärd.

2. I vilken mån brist på utformning av informationssäkerhet med avseende på behörighetskydd bidrar till avsiktlig eller oavsiktlig spridning av patientens personuppgifter, så att patientens integritet skadas.

3. I vilken mån tillverkaren av MTP har ansvar för att i sin riskhantering balansera och säkerställa patientens rättmätiga skydd mot att dels drabbas av fysisk skada och dels att få sin integritet kränkt.

4. I vilken mån myndigheterna kan förtydliga regelverket för *MT-data* i dess väg från registrering av biologiska parametrar hos patienten till undersökningsresultat i en journaluppgift.

Vi kan konstatera att det finns olika uppfattningar mellan Datainspektionen (DI) och vårdens myndigheter i synen på dessa frågor. Problematiseringen på myndighetsnivå kan formuleras som: Hur ska de komma överens, så att de tillsammans proaktivt kan vägleda vårdorganisationerna och tillverkarna av MTP i hanteringen av integritetsfrågor i den dagliga praktiska användningen av MTP inom sjukvården?

Det är mycket angeläget att MTP även skyddar patientens integritet, men att det ska ske i balans med upprätthållandet av den fysiska patientsäkerheten.

Framtidsperspektivet innehåller mer MTP i patientens bostad och i den kommunala omsorgen. Samverkan mellan kommuner och landsting/regioner ökar. Införandet av molntjänster med stora databaser, ofta fysiskt lokaliserade utanför Sveriges gränser, kopplade till MTP kommer sannolikt att bli vardag. Tillverkare av MTP kommer i allt större omfattning att erbjuda appar eller webbtjänster kopplade till sina produkter. Patienter rör sig allt oftare mellan olika vårdgivare i flera olika länder, vilket ställer krav på nationell och/eller EU-samverkan.

Avsnitt II:

Riktlinjer och rekommendationer till aktörerna inom området

Målsättning

Denna rapport gör inte anspråk på att ge tillräckliga svar på alla ovanstående problembeskrivningar. Målsättningen är dock att försöka bringa en viss klarhet och ge förslag på konkreta lösningar avseende en del av frågeställningarna. Vi hoppas att detta kommer att leda till en ökad förståelse hos de olika aktörerna inom området för den problematik som LfMT upplever vad gäller tillämpningen av gällande regelverk. Vi ser gärna att man med stöd av vår ursprungliga rapport Del 1 och denna Del 2 kan få underlag att ta initiativ till samarbeten, konsensus och förbättringar avseende utformning och hantering av informationssäkerheten i MTP.

De jurister vi varit i kontakt med är överens om att ordalydelsen i PDL 1 kap. 1 § om ”Vårdgivarens behandling av personuppgifter inom hälso- och sjukvården” innebär att PDL även omfattar *MT-data*. PDL är mycket omfattande avseende hur journalinformation ska hanteras. Många jurister anser att PDL är bristfällig med avseende på hur personuppgifter som inte är journalinformation ska hanteras. Det innebär att personuppgifter som inte är journalinformation (t. ex. *MT-data*) övertolkas till att även de ska hanteras som journalinformation.

PDL missleder redan i sina inledande definitioner (1 kap. 3 §) läsaren att tro att det är den tekniska miljön som avgör om informationen är en journalhandling eller ej. Vid vård av patienter ska det enligt 3 kap. 1 § patientdatalagen föras patientjournal. Skyldighet att föra journal gäller främst den som har legitimation inom hälso- och sjukvården eller tandvården. I SOSFS 2008:14 förtydligas det i 3 kap. 4 § att det tydligt ska framgå vilken person som svarar för respektive journaluppgift, oavsett teknisk miljö som journalhandlingen hanteras i.

Journalinformation ska vara väsentlig. Det är den journalförande personens uppgift att bedöma informationens relevans och om den ska journalföras eller ej. Överdokumentation i patienten journal innebär också en risk för patientsäkerheten. När *MT-data* blir undersökningsresultat i journalen så föreskriver PDL att den ska sparas i minst 10 år. Sen är det IVO som äger beslutet om den kan förstöras eller ej.

PUL ger en betydligt mer relevant vägledning om hur *MT-data* kan hanteras. Bland annat påpekas i § 9h att man är skyldig att blockera eller utplåna artefakter, d. v. s. sådana personuppgifter (i detta fall *MT-data*) som är felaktiga eller ofullständiga, och i § 9i att *MT-data* ska förstöras när den inte längre används. Hälso- och sjukvården hanterar dagligen mycket stora volymer *MT-data*. I väntan på att PDL revideras så rekommenderar LfMT att man använder PUL som stöd i hur *MT-data* ska behandlas. En rekommendation som många av vårdens aktörer och några jurister tycker är intressant och som de anser bör vidareutvecklas. Denna rapport Del 2 är en vidareutveckling av detta synsätt. Del 2 avser också vara ett stöd att hantera *MT-data* enligt PDL till en rimlig nivå.

Litteratursökning avseende informationssäkerhet och MTP

I samband med framställandet av denna rapport genomfördes en litteraturstudie. Studien syftar till att identifiera relevanta publikationer inom området MTP och informationssäkerhet.

- Vad är känt avseende skydd av liv och hälsa i kombination med skydd av patientens integritet hos MTP?
- Finns det exempel där skydd av liv och hälsa har åsidosatts p.g.a. av informationssäkerhetsåtgärder eller exempel där patientens integritet har blivit kränkt via MTP?

Artikelsökningen omfattar de senaste 10 åren (år 2005 – 2015) och genomfördes i PubMed. Huvudfrasen i artikelsökningen var: ”*Medical devices and its information security and their effectiveness or harm to the patient*”. Sökningen resulterade i 1834 artiklar. Dessa artiklar filtrerades genom att begreppen ”*Medical devices and information security*” kombinerades i tur och ordning med följande termer; ”*Confidentiality*”, ”*Integrity*”, ”*Access control*”, ”*Harm*”, ”*Patient integrity*”, ”*Consequence*” och ”*Information availability*”.

Artikelsökningen resulterade i 151 artiklar för rubrikgenomgång. Rubrikgenomgången identifierade 9 st relevanta publikationer för abstraktgenomgång. Två (2) artiklar lästes i sin helhet:

- Fernández-Alemán, 2013-01-08, ”*Security and privacy in electronic health records: a systematic literature review*”.
- Cucoranu IC, 2013-03-14, ”Privacy *and security of patient data in the pathology laboratory*”.

Slutsatsen från litteraturstudien är att:

- MTP kopplade till IT-system innehåller känsliga personuppgifter.
- Dessa personuppgifter bör skyddas för att H&S-vården ska behålla allmänhetens förtroende.
- MTP kopplade till IT-nätverk bör skyddas enligt liknade principer som gäller för en ansluten PC.
- Informationssäkerheten, i omsorg om patienten, bör utformas så att behörig vårdpersonal får ”tillgång till erforderlig information i rätt tid”.
- Om inte tillgång ges den normala vägen, så bör det finnas ett alternativt sätt att akut få tillgång till informationen.
- Riskanalys med alla berörda parter bör genomföras innan första användningstillfället.
- Frågeställningen om hur patientens integritet och säkerhet ska hanteras bör vidareutvecklas för målgruppen sjukvårdspersonal och hälso- och sjukvårdsorganisationer.
- Mer forskning och utveckling behöver göras inom området.

Majoriteten av artiklarna gav förslag på olika arkitekturer och tekniker för att höja informations-säkerheten och integritetsskyddet runt känsliga personuppgifter. Vi fann inga erfarenhetsbaserade artiklar om integritetsskydd i MTP och dess effekter i vårdverksamheten eller konsekvenser avseende skydd av liv och hälsa och skydd av patientens integritet för patienter direkt eller indirekt kopplade till MTP.

Generella riktlinjer

Medicinteknisk säkerhet

En MTP är enligt LMP och tillverkarens uppgifter avsedd för en specificerad medicinsk användning. Den ska i klinisk evidens uppvisa en klinisk nytta som speglar det av tillverkaren utpekade användningsområdet. En MTP ska vara lämplig för sitt avsedda användningsområde och uppnå de prestanda som tillverkaren har preciserat.

Regulatoriskt så ska en MTP, enligt Läkemedelsverkets föreskrifter, uppfylla *väsentliga krav* om säker och ändamålsenlig teknik som tillgodoser kraven på skydd av liv och hälsa. Tillverkaren ska bifoga en signerad *försäkran om överensstämmelse* att man följer väsentliga krav avseende att:

- Produkterna ska konstrueras och tillverkas så att de inte äventyrar patienternas kliniska tillstånd eller säkerhet eller användarnas eller andra personers hälsa och säkerhet när de används under avsedda förhållanden och för avsedda ändamål.
- Nyttan ska vida överstiga den risk som patienten utsätts för.
- Identifierade risker ska av tillverkaren;
  - i första hand elimineras via bättre konstruktion av MTP,
  - i andra hand begränsas genom skyddsmekanismer eller

- i tredje hand informeras om så att användaren är medveten om den risk man tar vid användning av MTP, så att man kan göra ett val om annat tillvägagångsätt.

Den kliniska evidensen ställs mot risken att skada i en *risk-/nyttobalans*. EU:s medicintekniska direktiv (MDD) ger ett tydligt besked att MTP ska förses med ”väsentligt skydd för liv och hälsa”. Pågående revidering av MDD (där direktivet bl.a. lyfts upp till att bli en EU-förordning) handlar om att stärka upp tillverkarens bevisbörda om klinisk evidens och ständig riskhantering under produktens hela livscykel. MDD närmar sig därmed regelverket för tillverkning av läkemedel.

Patientsäkerhet

Patienten ges i PSL en rättighet om en säker hälso- och sjukvård. Vårdgivaren har en skyldighet och organisatoriskt ansvar att via ledningssystem bedriva ett systematiskt patientsäkerhetsarbete med riskhantering och egenkontroll.

Som stöd till vårdgivaren och dess verksamhetschefer tillhandahåller SKL patientsäkerhetshandbok ”Riskanalys och Händelseanalys” (ISBN 978-91-7585-237-9). Den anger för gradering av ***allvarlighetsgrad*** respektive ***konsekvens*** i samband med riskanalys följande skala:

4.	**Katastrofal**	Dödsfall/självmord eller bestående stor funktionsnedsättning
3.	**Betydande**	Bestående måttlig funktionsnedsättning eller förlängd vårdepisod alt förhöjd vårdnivå för tre eller fler patienter
2.	**Måttlig**	Övergående funktionsnedsättning eller förlängd vårdepisod alt förhöjd vårdnivå för en eller två patienter
1:	**Mindre**	Obehag eller obetydlig skada

En av hörnstenarna i hälso- och sjukvårdens regelverk är att nyttan av den vård som ges ska vida överstiga den risk som vården innebär.

IT-säkerhet

IT-säkerhet, som beskrivs i standardiseringsfamiljen SS-ISO/IEC 27000, är de åtgärder som vidtas för att hindra att information läcker ut, förvanskas eller förstörs och för att informationen ska vara tillgänglig när den behövs. Den villar på tre grundläggande krav:

- **Konfidentialitet** [Confidentiality] Har du rätt att ta del av informationen?
  - Vårdrelation med patienten och i vissa fall patientens samtycke.
  - Behörighetskontroll.
  - Manuell eller en eller två faktorers autentisering.
- **Riktighet** [Integrity] Kan du lita på att informationen är rätt och att den inte är förvanskad eller en artefakt?
- **Tillgänglighet** [Availability] Är informationen tillgänglig när den behövs för behörig person?
  - Inom begreppet ”Tillgänglighet” förekommer också krav på **Spårbarhet** [Traceability] – Vem har tagit del av informationen och när?

IT-säkerhet handlar om:

- Infrastruktur för teknik och informationshantering.
- Utformning av IT-plattformens arkitektur och informatik d.v.s. plattformar för klient, servrar och kommunikation.
- Policyer för tekniska säkerhetskrav och rutiner med syfte att vidmakthålla IT-säkerheten.
- Aktiviteter avseende utformning av hårdvara, programvara, PC-klienter, servrar, databaser, behörighetsskydd, segmentering, brandväggar, kryptering av data, säkerhetskopiering av informationen, virusskydd och patch-uppgraderingar och dylikt.
- Praktiska åtgärder som syftar till att säkerställa ovanstående grundläggande krav på IT-säkerhet.

Dessa åtgärder har det gemensamt att de syftar till att både proaktivt och reaktivt skydda informationen och dess behandling.

Informationssäkerhet

Informationen ska vara skyddad så att den inte avsiktligen görs tillgänglig eller avslöjas för obehöriga eller utnyttjas på ett otillåtet sätt. Informationssäkerheten syftar till att skydda individens integritet. Riskanalys avseende informationssäkerhet syftar till att visa graden av **konsekvens** (vilket är informationssäkerhetens motsvarande benämning för patientsäkerhetens *allvarlighetsgrad*) för individen om informationen sprids otillbörligt. Nedanstående skala har sitt ursprung från Samverkansgruppen för informationssäkerhet (SAMFI), vilken består av ett antal myndigheter som alla har ett särskilt ansvar för samhällets informationssäkerhet. Det finns ingen nationell konsensus inom landsting/regioner motsvarande SKL patientsäkerhetshandbok. Region Skåne definierar som exempel dem enligt följande:

4. **Mycket allvarlig** Information där förlust av konfidentialitet innebär allvarlig/katastrofal negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ, speciellt om personen har en skyddad identitet.
   - Endast behöriga får tillgång till informationen.
   - Sekretess enligt Offentlighets- och sekretesslagen (OSL).
   - Information som omfattas av särskild lagstiftning, t.ex. PDL.

3. **Allvarlig** Information där förlust av konfidentialitet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
   - Personuppgifter i allmänhet eller som enligt PUL är att betrakta som känsliga.
   - Uppgifter av intern karaktär vilka endast egen personal bör ha tillgång till.

2. **Lindrig** Information där förlust av konfidentialitet innebär måttlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.

1. **Försumbar** Information där det inte föreligger krav på konfidentialitet, eller där förlust av konfidentialitet inte medför någon eller endast försumbar negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
   - Allmän och öppen information som utan skaderisk kan utlämnas till utomstående eller allmänheten.

En informationssäkerhetsriskanalys bör genomföras på alla tre perspektiven konfidentialitet, riktighet och tillgänglighet. Det pågår omfattande arbeten inom ett flertal grupperingar i Sverige och i

landsting/regioner avseende utformning av riskanalys av informationssäkerheten. För att få tillgång till aktuella riktlinjer bör man kontakta *personuppgiftsombudet* inom respektive landsting/region för närmare information.

EU:s dataskyddsreform

EU:s *Dataskyddsreform* genomförs i form av nya lagar om personuppgiftsbehandling. Reformen är preliminärt planerad att träda i kraft 2018. Bakgrunden till den nya reformen är ett förslag till nya regler om dataskydd och personuppgiftsbehandling som presenterades av Europeiska kommissionen i mars 2012. Syftet var att modernisera reglerna i dataskyddsdirektivet från 1995 och få till stånd en mer enhetlig tillämpning inom EU. Förslaget till reform innehåller dels en generell *dataskyddsförordning*, dels ett särskilt *dataskyddsdirektiv* för brottsbekämpande myndigheter. Den generella dataskyddsförordningen innehåller, enligt Datainspektionen (DI), bland annat:

- Fler och mer preciserade definitioner av olika begrepp såsom samtycke, genetiska uppgifter, biometriska uppgifter, m.m.
- Tydligare rättigheter för enskilda; Rätten att begära att personuppgifter raderas, rätten att få åtkomst till sina personuppgifter för att föra över dem till en annan leverantör av elektroniska tjänster för kommunikation, m.m.
- Tydligare regler om ansvar för de som behandlar personuppgifter, främst personuppgiftsansvariga men också personuppgiftsbiträden. Det finns krav på så kallade konsekvensanalyser (*Privacy impact assessments*), inbyggda dataskyddsgarantier (inbyggd integritet; *Privacy by design*) samt skyldighet att anmäla eventuella incidenter till tillsynsmyndigheten.
- Regler om förstärkt samarbete mellan de olika EU-medlemsstaternas dataskyddsmyndigheter och en så kallad *One-stop-shop-mekanism*. Denna mekanism ska underlätta för sådana personuppgiftsansvariga som är verksamma i flera medlemsstater (till exempel internationella företagskoncerner) genom att de endast ska behöva vara i kontakt med en av de olika nationella tillsynsmyndigheterna, nämligen den i det land där koncernen har sitt huvudsakliga verksamhetsställe.

Rekommendationer om balans mellan skydd av liv & hälsa och patientens integritet

Den generella uppfattningen bland alla aktörer verksamma inom området är att det är viktigt att man balanserar kraven på åtgärder för skydd av individens integritet med kraven på väsentligt skydd för liv och hälsa. Det saknas dessvärre riktlinjer för hur man praktiskt ska förfara för att uppnå en god balans mellan dessa båda skyddsvärden. Beskeden som SI:s arbetsgrupp hittills har fått vid dialog med olika myndigheter och andra aktörer är att man ska säkerställa dem båda så långt som det låter sig göras.

I avsaknad av konkreta anvisningar och vägledning, föreslår arbetsgruppen nedanstående rekommendationer att användas fram till dess att våra myndigheter kommer med tydliga besked:

A. Om det inte finns någon konflikt mellan att genomföra nödvändiga åtgärder för skydd av ”Liv och hälsa” och föreskrivna åtgärder för skydd av ”Patientens integritet”, rekommenderar vi att de genomförs fullt ut. Viktigt är dock att de åtgärder som genomförs inom respektive område också är föremål för riskanalys där båda aspekterna ovan vägs in, så att skyddsåtgärderna inte i sig innebär införande av nya risker för ”Liv och hälsa” och/eller ”Patientens integritet”.

B. Råder det en konflikt mellan att genomföra nödvändiga åtgärder för skydd av ”Liv och hälsa” och åtgärder för ”Patientens integritet” så ska åtgärderna balanseras, enligt nedanstående förslag på modell för riskbalansering.

Modell för riskbalansering

LfMT rekommenderar att tidskriterier används för balansering mellan skydd av liv och hälsa och patientens integritet.

För att uppnå en balans mellan skydd av ”Patientens integritet” och skydd av ”Liv och hälsa” rekommenderar LfMT att bedömningen sker mot följande tidskriterier, vilka har sitt ursprung inom ambulanssjukvården:

4. **Mycket stor** Akut tidskritiskt (livshotande). Åtgärd inom 15 minuter.
3. **Stor** Akut (inte livshotande). Åtgärd inom 60 minuter.
2. **Liten** Bråttom med rimliga väntetider. Åtgärd inom 4 timmar.
1. **Mycket liten** Väntetiden påverkar inte patientens tillstånd. Åtgärd kan dröja mer än 4 timmar.

Tidskriterierna ovan ska användas som riktlinje för hur lång tid det maximalt får ta att åtgärda eventuella hinder för åtkomst till patientens personuppgifter. När MTP innehåller mycket viktiga personuppgifter om en patient som vårdpersonalen behöver ha snabb åtkomst till, så bör behörighetsskyddet vara fristående från MTP. Se nedanstående resonemang om behörighetsskydd. Exempel på sådana MTP är hjärtövervakning på hjärtintensivvårdsavdelning (HIA) och blodgasanalyser på Förlossningen.

Inom ambulanssjukvården har man slutat att använda tidskriterierna, för att i stället uteslutande utgå ifrån patientens medicinska tillstånd. Bakgrunden till detta var att man upplevde att vårdpersonal tittade mer på klockan än på patientens faktiska tillstånd. Vi har dock valt att synliggöra tiden i syfte att de ska tjäna som riktmärken vid svåra avgöranden. Vi vill emellertid poängtera att det inte är dessa tidskriterier som är avgörande. Det är vårdpersonalens medicinska bedömning av patientens status som vägleder.

Det är Verksamhetschefen som har ansvaret att fatta beslut om riskbalanseringen när landstinget/regionen avser att förstärka informationssäkerheten på en befintlig MTP. Riskbalanseringen i den interna konstruktionen av MTP ansvarar tillverkaren för. Hur balanseringen ska utformas bör ingå i upphandlingen av MTP. Vårdgivare som följer standarden SS-EN 80001-1 om medicintekniska IT-nätverk hanterar riskbalanseringen enligt standardens processer.

Konfidentialitet avseende behörighetsskydd

Vårdgivaren ska fastställa bestämmelser och 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. Vårdgivare ska enligt PDL se till att vem som utnyttjat möjligheten till åtkomst till sådana patientuppgifter kan kontrolleras. Det är enligt lagen viktigt att både kunna verifiera och följa upp att den vårdpersonal som ges och har haft tillgång till patientens personuppgifter har en vårdrelation till patienten.

Ovanstående tidskriterier kan också användas som en generell anvisning om lämplig nivå på utformning av behörighetsskydd enligt följande kategorisering som föreslås av LfMT, vilken baseras på behovet av tillgång till patientdata:

4. Mycket stor Akut tidskritiskt (livshotande).
- Externt behörighetsskydd/skalskydd, d v s inget internt behörighetsskydd i MTP som verifierar personens identitet, innan tillträde ges till patientens personuppgifter.
- Synonymt patient-ID.

3. Stor Akut (inte livshotande).
- Internt behörighetsskydd med en-faktors-autentisering med krav på möjlighet att forcera behörighetskontrollen.

2. Liten Bråttom med rimliga väntetider.
- Internt behörighetsskydd med två-faktors-autentisering med krav på möjlighet att forcera behörighetskontrollen.

1. Mycket liten Väntetiden påverkar inte patientens tillstånd.
- Internt behörighetsskydd med två-faktors-autentisering utan krav på möjlighet att forcera behörighetskontrollen.

Definition av begrepp som används i kategoriseringen ovan:

- Med **externt behörighetsskydd/skalskydd** menas att behörighetskontrollen sker genom att en persons identitet kontrolleras på annat sätt än i aktuell MTP. Det kan vara aktuella tjänstgöringsregister där ansvarig chef tilldelar behörighet för åtkomst till personuppgifter i respektive MTP. Detta kan förstärkas med skalskydd i form av passagesystem till vårdlokalen.
- Med **internt behörighetsskydd** menas att behörighetskontrollen sker genom att en persons identitet kontrolleras internt i aktuell MTP, t. ex. via någon form av användarregister med respektive individs behörighet.
- Med **behörighetsskydd med en-faktors-autentisering** menas att behörighetskontrollen sker med enkel autentisering. Det innebär att en persons identitet kontrolleras genom att varje person vid anmodan anger sin personliga pinkod.
- Med **behörighetsskydd med två-faktors-autentisering** menas att behörighetskontrollen sker med stark autentisering. Det innebär att en persons identitet kontrolleras med två-faktors-autentisering. I fallet då SITHS tillämpas görs detta genom att varje person har ett personligt SITHS-kort som är kombinerat med en personlig pinkod.
- Med **synonymt Patient-ID** menas att personuppgifterna finns tillgängliga under pseudonym, till exempel ”Patient 4:2” (utläses som ”rum 4 och säng 2”) på bildskärm som lättillgängligt visar patientuppgifter/övervakningsdata inom den aktuella vårdenheten.

Som exempel på behörighetsskydd så bör man på system med risk för nivå 4: ”Mycket stor – Akut tidskritiskt (livshotande)”, inte använda något tekniskt behörighetssystem på aktuell MTP. Patientens integritet bör skyddas av extern manuell kontroll eller på annat sätt av vilka personer som ges tillträde till området där åtkomst till aktuell MTP är möjlig och av att det där endast finns behörig personal med patientrelation och som därmed har tillgång till personuppgifter nödvändiga för att kunna utföra sina arbetsuppgifter.

Den tekniska utformningen av behörighetsskydd på MTP ska tillgodose väsentliga krav i LMP. Detta ingår i tillverkarens ansvar.

Verksamhetschefen har ett stort ansvar för utformning och uppföljning av behörighetstilldelning och åtkomstkontroll. Den enskilda vårdpersonalen och teknisk personal har också ett stort ansvar i sin egenkontroll av vilka behörigheter man har och vilken information som man tar del av samt att aktivt förhindra oavsiktlig spridning av patienters personuppgifter.

I utformningen av behörighetssystem så måste man vara medveten om att patienten aktivt har sökt vård och därmed förväntar sig att vårdorganisationen använder den information som finns om dem till deras förmån. Alla bör därför hjälpas åt att med att skapa förutsättningar så att informationen finns tillgänglig när den behövs i vårdtillfället.

Riktighet och Tillgänglighet

Balanseringen av IT-säkerheten för att garantera informationens riktighet och tillgänglighet handlar om utvecklingen av standardiserade teknikplattformar och processer för utveckling och underhåll av IT-miljön.

Det bör utvecklas MT-anpassade plattformar för klient, servrar och kommunikation. Parallellt med dessa bör man fastställa policies för tekniska säkerhetskrav och rutiner för att vidmakthålla IT-säkerheten. Tillverkarna av MTP bör inta ett mer proaktivt förhållningssätt. Utvecklingen är att de för närvarande går från egentillverkad mjukvara till att använda standardiserade IT-komponenter från stora underleverantörer som t. ex. Microsoft och Adobe. Vi vet att dessa komponenter löpande får uppdateringar. Tillverkarna bör därför i sina riskanalyser i förväg godkänna dem och inte som nu reaktivt granska dem och sedan införa dem långt efter det att potentiella säkerhetsbrister har blivit identifierade.

Ovanstående tidskriterier bör även tjäna som riktmärke för områdena riktighet och tillgänglighet. Om avsedd användning av MTP är att hantera livshotande situationer hos patienten så indikerar ovanstående modell för balansering att det är mycket angeläget att säkerhetsbrister snabbt åtgärdas. Konsekvenserna för patienten vid ett e-virusangrepp kan i dessa fall vara avgörande om denne drabbas av vårdskada eller ej. Det finns idag leverantörer av livsviktig MTP som tar flera månader på sig att godkänna brådskande uppdateringar. Detta förhållande är djupt otillfredsställande.

MT-branschen måste hjälpas åt och arbeta för att vända på perspektivet, så att hanteringen av IT-säkerheten går från ett reaktivt till ett proaktivt förhållningssätt.

Biologisk information och dess väg som MT-data till journaluppgift

I syfte att konkretisera och exemplifiera tillämpningen av begreppet *MT-data,* så följer här ett fiktivt patientfall där läsaren får följa en hjärtpatients väg genom ett förenklat vårdprogram; ”Patient med diffusa bröstsmärtor”.

I det första avsnittet beskrivs hur patientens biologiska personuppgift EKG registreras av MTP och resulterar i *MT-data*, från vilka uppgifter/data av väsentliga för den fortsatta vården dokumenteras i patientens journal och därmed utgör ett undersökningsresultat i journalen. Observera att exemplet är förenklat och inte helt i överensstämmelse med gängse vårdpraxis.

I det andra avsnittet beskrivs vår tolkning av hur SoS och IVO utifrån begreppet ”Allmän handling” betraktar icke bedömd patientinformation från MTP, vilken vi i denna rapport benämner *MT-data*.

I det tredje och avslutande avsnittet tolkar vi vårt fiktiva patientfall med tillämpning av vår definition av begreppet *MT-data*.

Exempel - Patient med diffusa bröstsmärtor

1. Rutin-EKG tas på patienten vid besök på vårdcentralen.
2. Efter godkännande av behörig vårdpersonal lagras EKG:et i landstingets EKG-databas.
3. Den medicinska bedömningen av EKG-undersökningen förs in i patientens journal.
4. En tid därefter rycker ambulans ut till patienten som upplever diffusa bröstsmärtor. Ambulanspersonalen tar ett EKG som omgående skickas in till sjukhuset.
5. På sjukhuset jämförs ambulansens EKG med befintligt EKG från vårdcentralen i EKG-databasen.
6. Vårdpersonal tar ställning till ambulans-EKG:et och ger behandlingsråd till ambulansens personal, samt skriver in en anteckning i patientens journal.
7. Patienten anländer till sjukhusets Akutmottagning eller direkt till HIA, där ett nytt EKG tas. Beslut fattas om inläggning på HIA, samt notering sker i patientens journal.
8. Inläggning på HIA där patienten kopplas upp på hjärtövervakningsanläggning via EKG-modul. Patientens EKG övervakas löpande och av både vårdpersonal och larmkriterier i övervakningssystemet. EKG:t lagras temporärt under vårdtillfället i övervakningssystemets interna EKG-databas. Den äldsta delen av EKG-kurvan raderas successivt automatiskt när vårdtiden överskrider det minnesutrymme som är avsatt i systemet för den temporära lagringen av EKG. (D.v.s. att om utrymmet t. ex. är dimensionerat för tre dygn, så raderas EKG successivt från dygn ett när monitoreringen går in på dygn fyra o.s.v.).
9. Akut larm om plötslig och allvarlig förändring av patientens EKG-signal skickas ut till vårdpersonal på HIA. Larmet går både ut till bärbara larmmottagare och visas på enhetens övervakningsskärmar.
10. Medicinskt ansvarig kardiolog kontaktas av vårdpersonal, som kopplar upp sig från PC på Hjärtmottagningen (eller på en annan plats) för att ta del av patientens EKG-status. Ger via telefon ansvarig HIA-sjuksköterska riktlinjer om behandling.
11. Behandling av det akuta tillståndet påbörjas.
12. Effekten av behandlingen följs upp via patientens EKG på övervakningssystemets bildskärmar, samt genom analys av lagrad realtidsanalys i närtid av EKG och datortolkade arytmier.
13. Patienten lämnar det akuta tillståndet och kopplas till telemetriövervakning av EKG.
14. Patienten testas i både gång och trappträning för att se om hjärtat har stabiliserat sig.
15. Lagrat EKG i övervakningsutrustningen analyseras. De delar från patientens vårdtillfälle på HIA som bedöms som väsentliga för att komplettera övrig journalinformation förs in i journalen. Därefter raderas all övriga EKG-data från detta vårdtillfälle, då den inte längre anses behövlig.
16. Diagnostiskt EKG tas, vilket används som underlag för att skriva ut patienten från HIA. Utskrivningsanteckningar skrivs in i journalen om de är av avgörande betydelse.
17. Patienten kommer på återbesök på Hjärtmottagningen. Diagnostiskt EKG tas, vilket lagras i EKG-databasen.
18. Detta EKG jämförs med lagrat EKG från HIA-utskrivningen i vårdgivarens EKG-databas.
19. Resultatet av EKG-undersökningen förs in i patientens journal.

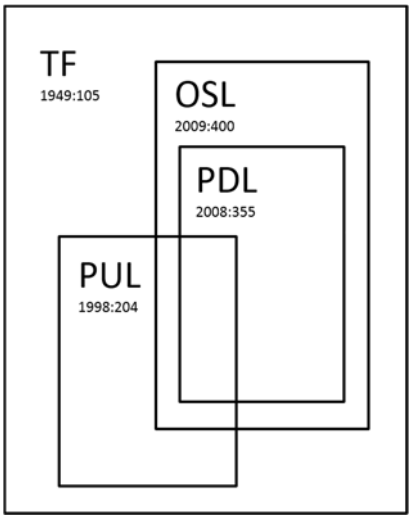
Vad är MT-data och när blir MT-data en Journalhandling?

Inför arbetsgruppens ovan nämnda möte med representanter för SoS och IVO hade myndigheterna innan mötet samrått med LV om hur man ska betrakta information från MTP, d v s det vi benämner *MT-data*. Vi redovisar i detta avsnitt vår sammanfattning av deras synpunkter på begreppet *MT-data*.

Det finns i huvudsak fyra lagar som berör informationshanteringen inom ***offentlig*** hälso- och sjukvård:

- **Tryckfrihetsförordningen (TF)**, vilken ligger som ett grundläggande regelverk för all medicinsk informationshantering inom offentlig förvaltning.
  - Vad som är en *Allmän handling* framgår av TF 2 kap. 3 §.
  - Vad som är en *Upprättad handling* framgår av TF 2 kap. 7 §.
  - Det åligger respektive landstingsarkivarie att upprätta ett *Arkiv- och gallringsreglemente*. Generellt bör det lokalt finnas ett gallringsbeslut för varje arkiv eller register med *upprättade handlingar.*
- **Offentlighets- och sekretesslagen (OSL)**
  - Denna lag innehåller bestämmelser om myndigheters och vissa andra organs handläggning vid registrering, utlämnande och övrig hantering av allmänna handlingar.
  - Lagen innehåller vidare bestämmelser om *tystnadsplikt* i det allmännas verksamhet och om förbud att lämna ut allmänna handlingar. Dessa bestämmelser avser förbud att röja uppgift, vare sig detta sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Bestämmelserna innebär begränsningar i yttrandefriheten enligt regeringsformen, begränsningar i den rätt att ta del av allmänna handlingar som följer av tryckfrihetsförordningen samt, i vissa särskilt angivna fall, även begränsningar i den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen.
- **Patientdatalagen (PDL)** ligger i sin helhet inom ramen för OSL.
- **Personuppgiftslagen (PUL)** berörs till vissa delar av innehållet i OSL och PDL.

Förhållandet mellan dessa fyra lagar kan förenklat åskådliggöras med nedanstående illustration:



Vidare så gäller att:

- **En patients personuppgift** är antingen en ”*allmän handling*” eller en ”*journalhandling*” vilka båda är sekretessbelagda.
  - SOSFS 2008:14 (som reglerar informationshantering och journalföring) ger direktiv om vad som ska räknas som ”*journalhandling*” respektive ”*allmän handling*”.
- Som **allmän handling** betraktas varje handling vilken har kommit in till eller är upprättad hos en statlig eller kommunal myndighet och som förvaras hos myndigheten. Handlingen kan vara i pappersform, innehållet i ett e-brev, ett ljud- eller videoband, en CD eller en diskett, och så vidare.
  - Vissa handlingar blir allmänna först om och när de omhändertas för arkivering. Det gäller sådana minnesanteckningar, utkast och koncept som ej har expedierats. Dessa skall ej heller, efter den tidpunkt då de är att anse som upprättade, anses som allmän handling hos den aktuella myndigheten om de inte arkiveras. Med minnesanteckning avses promemoria och annan uppteckning eller upptagning som har kommit till endast för ärendes föredragning eller beredning, dock ej till den del den har tillfört ärendet sakuppgift. Utkast

eller koncept till myndighets beslut eller skrivelse och annan därmed jämställd handling som ej har expedierats anses ej som allmän handling, såvida den ej tas om hand för arkivering (TF 2 kap. 9 §).

- **En handling anses som upprättad** hos myndighet när den har expedierats, justerats eller på annat sätt färdigställts. Hör den till ett ärende, blir den allmän senast när ärendet är färdigt.
  - Dock gäller för diarium, journal samt sådant register eller annan förteckning som förs fortlöpande, att handlingen anses upprättad först när den har färdigställts för anteckning eller införing i journalen/registret (TF 2 kap. 7 §).
- **En upprättad handling** som behövs för god vård, d. v. s. för att upprätthålla patientsäkerheten, ska enligt SoS journalföras.
- Enligt SOSFS 2008:1 (som reglerar användning av MTP) så motsvaras det som vi benämner ”*MT-data*” närmast av begreppet ”*Information”* från MTP.

Avseende privat hälso- och sjukvård faller de båda förstnämnda lagrummen ovan (TF och OSL) bort, såvida inte uppdraget kommer från en offentlig vårdgivare.

Ett exemplifierande resonemang om en EKG-kurva leder då till följande slutsatser:

- En EKG-kurva som visas i realtid på en bildskärm är **inte** en ”*upprättad handling*”.
- Om kurvan varit lagrad under en längre tid, kan den anses ”*arkiverad”* och har därmed passivt ”*fastställts*” och blir en ”*upprättad handling*”.
- Om någon information i EKG-kurvan (t.ex. en ST-höjning) anses väsentlig för den fortsatta vården av patienten, så ska den journalföras som ”*undersökningsresultat*” i patientens journal.

Tolkning av exemplet ”Patient med diffusa bröstsmärtor”

LfMT tolkar därför informationsklassningen i vårt exempel ovan, mot bakgrund av ovanstående centrala begrepp, enligt följande:

- En individs anatomiska status och dess biologiska signalnivåer utgör ursprung till ***personuppgifter***, vilka ännu inte är registrerade av någon MTP.
- Biologiska signaler som via sensorer är registrerade av MTP är *MT-data (Information lagrad i och/eller vidarebefordrad från en MTP),* vilka i egenskap av personuppgifter är sekretessbelagda.
- *MT-data* kan anses som ***”icke upprättad handling”***.
- En ***”icke upprättad handling”*** lagrad i en MTP är *MT-data* fram till annat beslutas av vårdpersonal efter granskning av den lagrade informationen.
- En ***”icke upprättad handling”*** i form av *MT-data* lagrad i en MTP blir en ***”upprättad handling”*** när den färdigställs för anteckning eller införing i patientens journal, eller när beslut om fortsatt arkivering tagits.
- *MT-data* lagrad i en MTP, vilken behövs för god vård, ska journalföras när legitimerad vårdpersonal bedömer den som väsentlig i vården av patienten.
- Väsentlig *MT-data* journalförs som ***”undersökningsresultat”*** i patientens journal och hanteras därefter som *journalhandling*.
- *MT-data* som inte journalförs ska förstöras när den ej längre behövs (*Det bör finnas ett* ***gallringsbeslut*** *från landstingets/regionens arkivmyndighet).*

De lagrum som blir aktuella för respektive kategori av data:

- För *MT-data* tillämpas lagrum PUL
- För *Journalhandling* tillämpas lagrum PDL

Ovanstående resonemang tillämpat på det inledande exemplet med en patient med diffusa bröstsmärtor kommer då att resultera i följande slutsatser:

1. *Rutin-EKG tas på patienten vid besök på vårdcentralen*.
   - Rutin-EKG:t från vårdcentralen är initialt MT-data. - ***”Icke upprättad handling”.***

2. *Efter godkännande av behörig vårdpersonal lagras EKG:et i landstingets EKG-databas*.
   - Vårdpersonalen godkänner att kvalitén på EKG:t är tillfyllest för att lagras i EKG-databasen. EKG:t som lagras i landstingets EKG-databas är MT-data. - ***”Upprättad handling”.***

3. *Den medicinska bedömningen av EKG-undersökningen förs in i patientens journal*.
   - Ansvarig vårdpersonal avgör om EKG-kurvorna ska sparas i patientens journal tillsammans med det medicinska utlåtandet. EKG-kurva och/eller utlåtande om EKG som sparas i journalen är ett ***”undersökningsresultat”*** och utgör en journalhandling. EGK:t vilken sparas i EKG-databasen är MT-data. - ***”Allmän handling”***. I de fall där uthopp sker från patientens journal till EKG-databasen, så ska även EKG-kurvan hanteras som en journalhandling - ***”Undersökningsresultat”***.

4. *En tid därefter rycker ambulans ut till patienten som upplever diffusa bröstsmärtor.*
   - Ambulanspersonalen tar ett EKG som omgående skickas in till sjukhuset. Ambulans-EKG:t är MT-data - ***”Icke upprättad handling”***.

5. *På sjukhuset jämförs ambulansens EKG med befintligt EKG från vårdcentralen i EKG-databasen*.

6. *Vårdpersonal tar ställning till ambulans-EKG:et och ger behandlingsråd till ambulansens personal, samt skriver in en anteckning i patientens journal*.
   - Det medicinska utlåtandet av EKG:t och eventuell råd, till ambulanspersonalen om behandling av patient, är en journalhandling. Övrig hantering av EKG:t sker i enlighet med punkt 3 ovan.

7. *Patienten anländer till sjukhusets Akutmottagning eller direkt till HIA, där ett nytt EKG tas. Beslut fattas om inläggning på HIA, samt notering sker i patientens journal*.
   - EKG:t som tas på Akutmottagningen ges en medicinsk bedömning hanteras i enlighet med punkt 3 ovan.

8. *Inläggning på HIA där patienten kopplas upp på hjärtövervakningsanläggning via EKG-modul. Patientens EKG övervakas löpande och av både vårdpersonal och larmkriterier i övervakningssystemet. EKG:t lagras temporärt under vårdtillfället i övervakningssystemets interna EKG-databas. Den äldsta delen av EKG-kurvan raderas successivt automatiskt när vårdtiden överskrider det minnesutrymme som är avsatt i systemet för den temporära lagringen av EKG. (D.v.s. att om utrymmet t. ex. är dimensionerat för tre dygn, så raderas EKG successivt från dygn ett när monitoreringen går in på dygn fyra o.s.v.)*
   - EKG från hjärtövervakningsanläggningens EKG-modul, och dess lagring i övervakningssystemets EKG-databas, är MT-data - ***”Icke upprättad handling”***.

9. *Akut larm om plötslig och allvarlig förändring av patientens EKG-signal skickas ut till vårdpersonal på HIA. Larmet går både ut till bärbara larmmottagare och visas på enhetens övervakningsskärmar*.
   - Akut larm om allvarlig förändring av patientens EKG-signal är MT-data - ***”Icke upprättad handling”***.

10. *Medicinskt ansvarig kardiolog kontaktas av vårdpersonal, som kopplar upp sig från PC på Hjärtmottagningen (eller på en annan plats) för att ta del av patientens EKG-status. Ger via telefon ansvarig HIA-sjuksköterska riktlinjer om behandling.*
    - Medicinskt ansvarig kardiolog för journalanteckning, när så erfordras, baserad på patientens EKG-status samt beslut om insatt behandling.

11. *Behandling av det akuta tillståndet påbörjas*.
    - Behandling påbörjas och HIA-sjuksköterskor för journalanteckningar om denna, när så erfordras.

12. *Effekten av behandlingen följs upp via patientens EKG på övervakningssystemets bildskärmar, samt genom analys av lagrad realtidsanalys i närtid av EKG och datortolkade arytmier.*
    - Direktövervakning av patientens EKG via övervakningssystemet och realtidsanalys i närtid samt datortolkade arytmier/utplockade avsnitt ur EKG-kurvan är MT-data - ”***Icke upprättad handling***”.

13. *Patienten lämnar det akuta tillståndet och kopplas till telemetriövervakning av EKG*.
    - Telemetriövervakning av EKG är *MT-data* - ”***Icke upprättad handling***”.

14. *Patienten testas i både gång och trappträning för att se om hjärtat har stabiliserat sig*.
    - Patientens mobilitet/stabilitet testas och dokumenteras med journalanteckning, när så erfordras.

15. *Lagrat EKG i övervakningsutrustningen analyseras. De delar från patientens vårdtillfälle på HIA som bedöms som väsentliga för att komplettera övrig journalinformation förs in i journalen. Därefter raderas all övriga EKG-data från detta vårdtillfälle, då den inte längre anses behövlig*.
    - De EKG-sekvenser från patientens vårdtillfälle på HIA som bedöms som väsentliga för att komplettera övrig journalinformation är journalhandling och förs in i journalen. Det kan ske, i enlighet med punkt 3 ovan, genom att man för in EKG-kurvorna i journalen eller att man lagrar EKG i en EKG-databas med möjlighet för uthopp från journalen till patientens EKG. Resterande EKG-kurvor raderas när de inte längre behövs i vårdtillfället.

16. *Diagnostiskt EKG tas, vilket används som underlag för att skriva ut patienten från HIA. Utskrivningsanteckningar skrivs in i journalen* om de är av avgörande betydelse.
    - Diagnostiskt EKG hanteras i enlighet med punkt 3 ovan.

17. *Patienten kommer på återbesök på Hjärtmottagningen. Diagnostiskt EKG tas, vilket lagras i EKG-databasen*.
    - Diagnostiskt EKG från Hjärtmottagningen hanteras i enlighet med punkt 3 ovan.

18. *Detta EKG jämförs med lagrat EKG från HIA-utskrivningen i vårdgivarens EKG-databas*.

19. *Resultatet av EKG-undersökningen förs in i patientens journal*.
    - Tolkningen av EKG:t och jämförelsen med tidigare lagrade EKG från HIA är ”undersökningsresultat” och utgör därmed även en journalhandling. Övrig hantering sker i enlighet med punkt 3 ovan.

I ovanstående tolkning så vill vi poängtera EU:s regulatoriska krav att **tillverkaren** ska ange den medicintekniska produktens ”***avsedda användning***”. Detta innebär, enligt LfMT, att om aktuell MTP är tillverkad i syfte att hantera journalhandlingar, så ska tillverkaren i sin konstruktion och underliggande riskanalys, se till att MTP kan uppfylla PDL. Om aktuell MTP däremot är avsedd att enbart hantera *MT-data* så ska tillverkaren, på motsvarande sätt, se till att aktuell MTP kan uppfylla PUL.

Fördjupning av checklistan från Del 1

I ovanstående avsnitt om informationssäkerhet beskrivs de åtgärder som ska vidtas för att hindra att information läcker ut, förvanskas eller förstörs och för att informationen ska vara tillgänglig när den behövs. Den villar på tre grundläggande krav:

- **Konfidentialitet** [Confidentiality] Har du rätt att ta del av informationen (sekretess)?
- **Riktighet** [Integrity] Är informationen korrekt och inte förvanskad?
- **Tillgänglighet** [Availability] Är informationen tillgänglig för behörig person och finns spårbarhet om vem som har tagit del av informationen och är informationen säkerhetskopierad?

IVO är tydlig med att medicinsk information ska vara tillgänglig när den behövs och att detta krav på tillgänglighet även gäller vid ett första fel på MTP. Detta är något som primärt vilar på tillverkaren och vårdgivaren; Att de tillsammans säkerställer tillgängligheten via reservrutiner i form av läskopia eller motsvarande. I detta ingår också rutiner för backup och dess återläsning av säkerhetskopierad information. Reservrutinerna ska testas innan första användning av MT-systemet och dessa tester ska regelbundet återkomma under MTP:s hela livscykel.

Standarden SS-EN 80001 om riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till MTP är tydlig med att informationssäkerheten via en riskanalys ska balanseras mot både patientsäkerheten och effektiv avsedd användning av MTP.

LfMT rekommenderar att balanseringen ovan utgår från att för *MT-data* tillämpas primära anvisningar som framgår ur PUL och för *MT-data* som blivit undersökningsresultat anvisningar avseende journalhandlingar i PDL. Detta finns förtydligat i bilagan till Del 1, ”*Checklista för att säkerställa en korrekt hantering av personuppgifter*”, som är ett hjälpmedel vilket tagits fram av LfMT till hjälp för förvaltare av MTP och MT-system med syfte att stödja hanteringen av personuppgifter i MTP i enlighet med gällande regelverk. Där anges också vilka lagrum som gäller inom respektive punkt.

PUL ålägger vårdgivaren att enbart behandla personuppgifter som är adekvata och relevanta i förhållande till ändamålen med behandlingen. Känsliga personuppgifter får behandlas, om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen och att personuppgifter inte får bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med dem.

Lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av:

a) de tekniska möjligheter som finns,
b) vad det skulle kosta att genomföra åtgärderna,
c) de särskilda risker som finns med behandlingen av personuppgifterna, och
d) hur pass känsliga de behandlade personuppgifterna är.

LfMT rekommenderar att samtycke från patienten inhämtas i samband med att vårdinsatsen med MTP påbörjas.

Ansvaret för att vidta lämpliga tekniska skydd och åtgärder delas av tillverkaren av MTP och användaren/Vårdgivaren. Standarden SS-EN 80001 rekommenderar att detta dokumenteras i ett ansvarsdokument mellan alla berörda parter innan första användningstillfället på patient.

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. Journaluppgift ska sparas i minst 10 år och kan förstöras först efter beslut av IVO.

Checklista

Checklistan nedan (Se även Bilaga 1 i Del 1) är avsedd som ett stöd för förvaltare av MTP och anslutna IT-system med syfte att ge konkreta direktiv för hanteringen av personuppgifter i MTP. Lokal MT- respektive IT-avdelning fungerar som stöd till berörd verksamhetschef i beredning och genomförande av beslut i dessa frågor.

Checklistan är tänkt att fungera som en interimslösning, som via en pragmatisk ansats tolkar kraven i nuvarande regelverk fram till dess att berörda myndigheter och övriga aktörer eliminerat nuvarande oklarheter.

1. Grunden i en korrekt hantering av personuppgifter i MTP är att det som ska mätas, bearbetas etc. sker med utrustning som är medicinskt lämplig för sitt ändamål. Det är viktigt att detta är verifierat med tillverkarens anvisningar för aktuell MTP. I samband med upphandling bedöms huruvida offererad MTP fyller sin funktion och hur personuppgifter hanteras i produkten.

   Lagrum LMP – Avsedd medicinsk användning (5 §) och väsentliga krav (6 §).

2. Avseende MTP som enbart visar *MT-data* i avidentifierad form, ska användarna vara medvetna om att det är upp till dem själva att fånga och koppla väsentlig information till aktuell patient för journalföring. Information om detta ges under utbildningen av användarna.

   Lagrum PUL – Avidentifierad innebär att det inte finns någon koppling, nyckel eller annan anordning som gör det möjligt att koppla informationen till en person (22 § och Prop. 1997/98:44). Avidentifierade uppgifter, i den mening detta begrepp används i integritetsskyddshänseende, omfattas inte av personuppgiftslagen. (Datainspektionen, diarie 2469-2014).

3. Visas pseudonymiserade *MT-data*, 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. Detta kontrolleras i samband med upphandlingen.

   Lagrum PUL – Graden av sekretess och åtkomst till nyckeln avgörs av hur pass känsliga de behandlade personuppgifterna är (Datalagskommittén, SOU 1997:39 och EU:s Artikel 29 - Arbetsgrupp för skydd av personuppgifter 0829/14/EN WP216).

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 eller i ett anslutet IT-system. Normalt täcks detta behov av personalens tystnadsplikt och graden av skydd bedöms utifrån avsedd användning av aktuell MTP.

   Exempelvis ska ett övervakningssystem på en IVA-avdelning alltid vara öppet så att information på bildskärmar och dylikt snabbt finns åtkomlig. D.v.s. det kan finnas risk för att obehörig ser information som denne enligt regelverket inte borde ha tillgång till. Avsedd användning av aktuell MTP/MIS och patientsäkerhetsaspekter medför dock att risken för obehörig

informationsåtkomst i detta fall kan accepteras. Patientens identitet bör dock, i enlighet med punkt 3 ovan, i möjligaste mån skyddas via pseudonymiserat ID.

Lagrum LMP – Avsedd medicinsk användning (5 §) och väsentliga krav (6 §).

Lagrum PUL – Riskanalys används för att balansera skydd av ”Liv och hälsa” mot skydd av ”Patientens integritet” (10 §, 18 §, 22 § och 31 §).

5. Patientens identitet ska på ett säkert sätt fastställas och verifieras när ID kopplas till *MT-data* som härrör från aktuell patient.

   Lagrum PUL – Verifiera patientens identitet med ID-handlingar (9 §).

6. Lagras *MT-data* med patient-ID, oberoende av var detta sker, så ska detta personregister anmälas till vårdgivarens personuppgiftsombud.

   Lagrum PUL – Den som är personuppgiftsansvarig ska se till att den registrerade patienten får information om personuppgiftsbehandlingen. Informationen ska innehålla upplysningar om vem som är personuppgiftsansvarig, ändamålet med behandlingen och andra uppgifter (9 §).

7. Visas *MT-data* med patient-ID så ska det säkerställas att endast behörig personal, med spårbarhet (manuellt eller elektroniskt) med avseende på vem, när och vad, tar del av *MT-data*. Vid integration med journalsystem, enligt punkt 12 och 15 nedan, bör spårbarheten den vägen hanteras av journalsystemet.

   Lagrum PUL – Den information som görs tillgänglig för behörig person ska loggas så att spårbarhet ges om vem som har tagit del av personuppgiften (9 §).

8. *MT-data* ska förstöras löpande när de inte längre behövs. Rutiner för detta implementeras i samband med installation av MTP.

   Lagrum PUL – Personuppgifter ska inte bevaras under en längre tid än vad som är nödvändigt (9 §).

9. Sker en bearbetning av *MT-data*, så ska metoden verifieras mot MTP-tillverkarens anvisningar. Detta kontrolleras under upphandlingen.

   Lagrum LMP – Väsentliga krav (6 §).

10. När vårdpersonal bedömer att *MT-data* är väsentlig att journalföras och därmed ska betraktas som journalhandling, så ska det ske enligt fastställda lokala riktlinjer om hur och när *MT-data* definieras som undersökningsresultat, samt genom integration blir tillgängliga som stöd till journalhandlingen.

    Observera att vid uthopp från journalsystem till integrerad MTP ska man **inte** inom MTP kunna nå *MT-data* från en annan patient än den som ursprungligen valts i journalsystemet. Detta **måste** kontrolleras vid upphandlingen.

    Lagrum PDL – Vid vård av patienter ska det föras patientjournal (3 kap. 1 §). En patientjournal ska föras för varje patient och får inte vara gemensam för flera patienter.

11. Undersökningsresultat bör journalföras i MTP vilken av tillverkaren är avsedd för att användas för att journalföra patientuppgifter.

    Lagrum LMP – Avsedd medicinsk användning (5 §) och väsentliga krav (6 §).

    Lagrum PDL – En patientjournal ska innehålla de uppgifter som behövs för en god och säker vård av patienten (PDL 3 kap. 1 § och SOSF 2008:14 6 §).

12. När man integrerar *MT-data* från MTP via IT-nätverk med journalsystem, så ska man vara säker på om överföringen av patientuppgifter sker via ett öppet eller slutet nät och skapa förbindelsen säkerhetsmässigt utifrån dessa förutsättningar. I samband med upphandlingen kravställs detta i samråd med den lokala IT-organisationen.

    Lagrum LMP – Tillverkaren av MTP ska i sina anvisningar (5 §) ange hur överföringen ska ske på ett säkert och ändamålsenligt sätt så att de väsentliga kraven (6 §) vidmakthålls.

    Lagrum PDL – En vårdgivare ska se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och kan kontrolleras (4 kap. 2 §). Vid uthoppsintegration, enligt punkt 14 och 15 nedan, sker det lämpligast i det journalsystem som uthoppet sker ifrån. Om annan vårdgivare tar del av personuppgifter uppstår en ***sammanhållen journalföring*** *(6 kap. 2 §) och därmed högre krav på informationssäkerhet.*

13. Om integrationen mellan MTP och journalsystem sker via ett öppet nät, så ska överföring av patientuppgifter genomföras på ett sådant sätt att ingen obehörig kan ta del av uppgifterna. Åtkomst till patientuppgifter ska i detta fall om möjligt regleras via stark autentisering. Se punkt 12 ovan.

    Lagrum LMP – Avsedd medicinsk användning (5 §) och väsentliga krav (6 §).

    Lagrum PDL – Stark autentisering är behörighetsskydd med två-faktors-autentisering där en persons identitet kontrolleras genom ett personligt SITHS-kort och en personlig pinkod. Överföring av information ska vara krypterad och spårbar (4 kap. och SOSFS 2008:14 1 kap. 3 §).

14. Integreras *MT-data* med journalsystem via integrationsmjukvara, ska man verifiera med tillverkaren av journalsystemet att integrationen uppfyller väsentliga krav för avsedd användning av uthopps- eller hybridintegration. Se förtydligande figur avseende integration nedan. Detta kontrolleras i samband med upphandlingen av mjukvaran.

    Lagrum LMP – Avsedd medicinsk användning (5 §) och väsentliga krav (6 §).

    Lagrum PUL – Information i MTP vilken inte är kopplad till journalsystem ska vara skyddade så att inte okontrollerad eller oavsiktlig åtkomst till informationen är möjlig (31 §).

    Lagrum PDL – Krypterad och spårbar överföring (4 kap.).

15. I samband med upphandlingen kravställs vilken åtkomst till journalsystemet som verksamhetschefen tillåter. Kraven skall klargöra om åtkomst ska ges enbart inom en vårdenhet, inom vårdgivaren eller mellan flera vårdgivare.

    Kravställningen baserad på verksamhetschefens beslut om åtkomst omfattar också hur en av patient begärd spärr ska hanteras i journalsystemet. Vid uthopp till MTP så är det journalsystemet som hanterar den av patient begärda åtkomstbegränsningen så att den också omfattar spärrad *MT-data*.

    Lagrum PDL – Innan uppgifter om en patient görs tillgängliga för andra vårdgivare genom sammanhållen journalföring, ska patienten informeras om vad den sammanhållna journalföringen innebär och om att patienten kan motsätta sig att uppgifter görs tillgängliga för andra vårdgivare genom sammanhållen journalföring (6 kap).

16. Det ska finnas praktiska rutiner inklusive anvisningar framtagna och kommunicerade till vårdpersonalen avseende hur man spärrar patientuppgifter i de fall där patienten har rättighet att införa en spärr. Man bör vara medveten om att det är mycket ovanligt att en patient önskar spärra *MT-data* eller undersökningsresultat från MTP. Patienter som har spärrat information önskar som regel få spärren hävd i en akut medicinsk situation för att ge vårdpersonalen tillgång till befintlig *MT-data.* Införandet av spärr och dess nödöppning av *MT-data* bör därför

förberedas och testas. Rutiner för detta kontrolleras och utarbetas eventuellt i samband med upphandlingen av MTP.

Lagrum PDL – Personuppgifter som dokumenterats för vården av patienter 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. I sådana fall ska uppgiften genast spärras (4 kap. 4 §).

17. Det ska finnas praktiska rutiner inklusive anvisningar framtagna och kommunicerade till vårdpersonalen för hur vårdgivaren inhämtar och dokumenterar patientens samtycke för sammanhållen journalföring. Detta täcks normalt av redan befintliga rutiner, men bör kontrolleras vid upphandlingen.

    Lagrum PDL – Se punkt 16 ovan.

18. Förstörande av patients journaluppgift lagrad i medicinska informationssystem (MIS) får ske först efter beslut av IVO om vad och vilken information i journalhandlingen som får förstöras.

    Lagrum PDL – På ansökan av patienten eller någon annan som omnämns i en patientjournal får IVO besluta att journalen helt eller delvis ska förstöras (8 kap. 4 §).

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 riskanalys baserad på tillverkarens anvisningar för aktuell MTP avseende dess funktion, egenskaper och prestanda. Syftet är att om möjligt minimera både risken för patienten att drabbas av vårdskada och risken för kränkning av sin integritet.

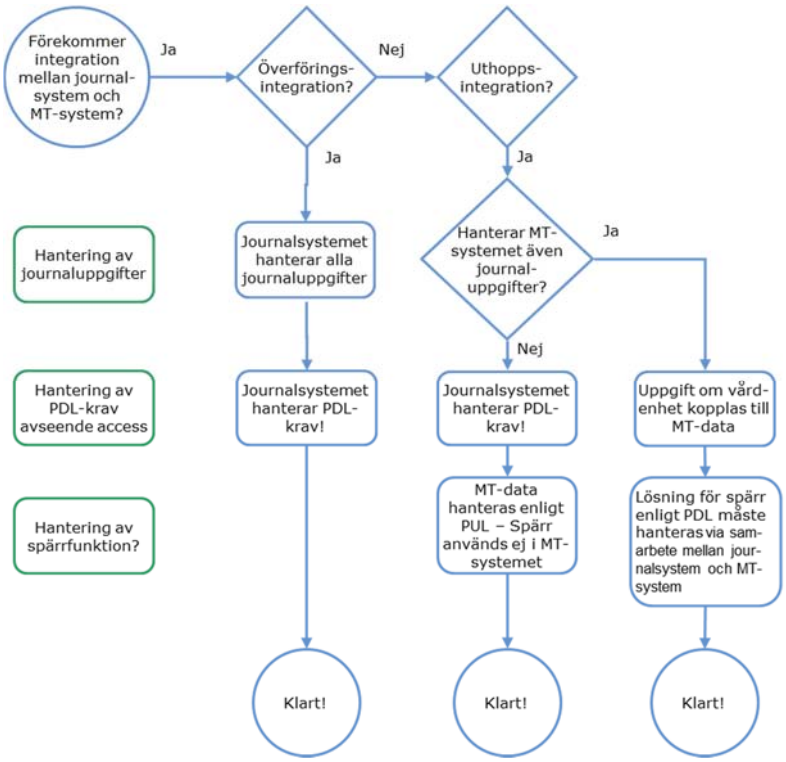
    Resultatet från tillverkarens riskanalys, vilket berör användandet av MTP, ska finnas med i tillverkarens anvisningar för MTP. Vid oklarheter kontaktas tillverkaren för att få visshet.

    Lagrum PSL – Hälso- och sjukvårdspersonalen är skyldig att bidra till att hög patientsäkerhet upprätthålls. Personalen ska i detta syfte genomföra riskanalyser där så är nödvändigt och till vårdgivaren rapportera risker för vårdskada samt händelser som har medfört eller hade kunnat medföra en vårdskada eller att patientens integritet kränks (PSL 6 kap. 4 §).

20. Verksamhetschefen är ansvarig för att anslutna IT- och behörighetssystem är säkra och lämpliga och får användas på patient. Lokal MT- respektive IT-organisation bör medverka i processen att ta fram och sammanställa ett lämpligt underlag för detta beslut.

    Lagrum LMP – Verksamhetschefen ansvarar för att endast säkra och medicinskt ändamålsenliga MTP, inklusive anslutna informationssystem, används på patienter. Verksamhetschefen ansvarar också för att MTP inklusive anslutna informationssystem är kontrollerade och korrekt installerade innan de används på patienter (SOSFS 2008:1, 3 kap. 6 § pkt. 1 och 3). För egentillverkad MTP gäller också att verksamhetschefen ska intyga, i en Försäkran om överensstämmelse, att denna i tillämpliga delar uppfyller de av Läkemedelsverket angivna väsentliga krav på MTP (SOSFS 2008:1, 5 kap. 6 §).

Förtydligande avseende integration



För fallet då de olika typerna av integration i figuren ovan kombineras, så har arbetsgruppen definierat begreppet *Hybridintegration, där hybrid* betyder "blandning" och *integration* betyder ”förening”.

Vid alla former av integration så är journalsystemet primärt huvudansvarigt för att tillhandahålla de tekniska lösningar som krävs för att leva upp till PDL. Om berörd MTP också har som avsedd användning att föra journal, så gäller detta krav även denna MTP.

Vid integration mellan MTP och journalsystem hanteras också frågan om när en patient begär åtkomstbegränsning för annan vårdenhet eller inom en annan vårdprocess hos samma vårdgivare. Det är mycket ovanligt att en patient vill spärra *MT-data*. (Vi känner endast till några få tillfällen. I samtliga fall handlade det då om spärr av röntgenbilder). LfMT anser att det inte är rimligt att de MTP som inte är journalsystem ska hantera spärr av *MT-data*. Spärr bör i dessa fall hanteras via patientens journal. Se punkt 15 ovan.

Rekommendationer

Här följer en sammanfattning av de fyra centrala områdena i den problemställning rapporten behandlar och LfMT:s rekommendationer för hantering av dem:

1. **I vilken mån utformningen av behörighetsskyddet inverkar negativt på effektiviteten i vårdarbetet och därmed risken att fysiskt skada patienten genom antingen en felaktig diagnos och behandling eller utebliven nödvändig medicinsk åtgärd.**

   1.1. Rekommendation:
   - Säkerställ att utformningen av användningen av MTP utgår från tillverkarens avsedda användning.
   - Säkerställ att vårdgivarens användning av patientens personuppgift utgår från de föreslagna kriterierna i avsnittet *Generella riktlinjer/Behörighetsskydd* ovan, så att man med hjälp av dessa balanserar patientens rättmätiga krav avseende både ”Liv och hälsa” och ”Patientens integritet”.

2. **I vilken mån brist på utformning av informationssäkerhet och dess behörighetskydd bidrar till avsiktlig eller oavsiktlig spridning av patients personuppgifter, så att patientens integritet skadas.**

   2.1. Rekommendation:
   - Patentens personuppgifter, inklusive *MT-data*, bör i möjligaste mån vara krypterade.
   - *MT-data* bör hanteras inom väl avgränsade och skyddade logiska områden (brandväggar och liknade lösningar)
   - Det ska finnas begränsade möjligheter att använda inbyggda kopieringsfunktioner hos ansluten datorutrustning (t. ex. blockering av kommandot <Ctrl> + <C>).
   - Vårdgivaren bör utbilda och ständigt medvetandegöra vård-, MT- och IT-personal om vårdens sekretessrutiner och hur man undviker att sprida *MT-data* till obehöriga.

3. **I vilken mån ansvarar tillverkaren av MTP för att i sin riskhantering balansera och säkerställa patientens rättmätiga skydd mot att drabbas av fysisk skada mot att få sin integritet kränkt?**

   3.1. Rekommendation:
   - Läkemedelsverket bör ge tillverkaren tydliga riktlinjer att i sin riskanalys identifiera och åtgärda risker för skydd av både ”Liv och hälsa” och ”Patientens integritet”.
   - Både tillverkare och vårdgivare bör utbilda och ständigt medvetandegöra sin personal om risker med informationshantering i MTP. De bör också arbeta för att skapa och implementera konstruktioner för lämpliga skydd av både ”Liv och hälsa” och ”Patientens integritet”, samt följa den utveckling som pågår inom informationssäkerhetsområdet och omsätta den till ny kunskap om hur man via tekniska konstruktioner kan undvika att av misstag sprida *MT-data* till obehöriga.

4. **I vilken mån myndigheterna kan förtydliga regelverket för *MT-data* på dess väg från biologiska parametrar hos patient till undersökningsresultat i en journaluppgift?**

   4.1. Rekommendation:
   - Myndigheterna SoS, IVO och LV bör analogt med ovanstående resonemang skapa och publicera instruktioner om hur man ska betrakta *MT-data* och när den ska definieras som journalhandling.
   - Socialdepartementet och Justitiedepartementet bör, i samband med EU:s pågående förändring av dataskyddsdirektivet, arbeta för att harmonisera lagrummen som reglerar informationsbehandling inom hälso- och sjukvården respektive i MTP med avseende på lagarna PSL, PUL, PDL och LMP.

Specifika krav på tillverkare och vårdgivare

Tillverkaren:

- Har ansvar att tillgodose höga krav på skydd av liv och hälsa hos medicintekniska produkter. Detta ansvar omfattar även informationssäkerheten.
- Ska tydligt ange om aktuell MTP är avsedd för att föra eller hantera journaluppgifter eller att integreras med annan MTP eller annat system avsett för journalföring (t. ex. via uthoppsintegration).
- Ska anmäla väsentliga problem och frågeställningar angående behörighetssystem och informationssäkerhet i sina produkter till Läkemedelsverket.

Vårdgivaren:

- Bör, enligt standarden SS-EN 80001-1, vara tydlig med att fråga tillverkarna om vilka begränsningar som finns i deras MTP med avseende på informationssäkerhet och behörighetsstyrning.
- Har, utifrån avsedd medicinsk användning, ansvaret för informationssäkerheten i hanteringen av personuppgifter, men har inte huvudansvaret för utformning och konstruktion samt implementering av integritetsskydd i MTP från externa tillverkare.
- Ska anmäla brister i behörighetssystem och informationssäkerheten till både Läkemedelsverket och tillverkaren av aktuell MTP.

Både tillverkaren och vårdgivaren:

- Måste förbättra balansen i MTP mellan integritetsskydd och skydd mot fysisk skada.
- Måste se till att utformning av åtkomst till information är lämplig för produktens avsedda medicinska användning.
- Bör gemensamt arbeta för att det utvecklas fler tekniska lösningar som, om möjligt, kan minimera alternativt eliminera problemen.
- Bör gemensamt arbeta för att skapa fora för möten med de berörda aktörerna som myndigheter, akademin, industrin, vårdorganisationer och patientorganisationer.
- Bör vara överens om att inget motsatsförhållande råder mellan krav på att skydda patienten från fysisk skada och krav på skydd av patientens integritet.

Förslag till fortsatt arbete

LfMT bör fortsättningsvis arbeta med att:

- Fokusera mer på hur man för MTP ska uppnå en god balans mellan integritetsskydd och skydd mot fysisk skada.
  - Lista vilka olika tekniska lösningar som finns för skydd av patientens integritet.
  - Bedöma hur väl de fungerar.

- Bredda nuvarande aktiviteter för utveckling av ”MT-klienter”, så att det även utvecklas MT-anpassade plattformar för servrar och kommunikation.
  - Ta fram MT-policies med tekniska säkerhetskrav och rutiner för att utveckla och vidmakthålla IT-säkerheten.

- Initiera samverkan med vårdens nationella IT-säkerhetsorganisationer och Swedish Medtech för att stimulera framtagandet av enhetliga nationella modeller för god informationssäkerhet vid användning av MTP.
  - Tillsammans med berörda parter ta ett initiativ till ett nationellt tvärprofessionellt forum.

  - Ta fram fler konkreta exempel på tekniska problem att hantera i detta forum.

- I dialogform med berörda myndigheter och departement; Läkemedelsverket, Socialstyrelsen, IVO, E-Hälsomyndigheten och Datainspektionen, driva frågorna om:
  - Att i samband med att MDD omvandlas till EU-förordning komplettera regelverket med anvisningar för både tillverkarna och vårdgivarna om hur informationssäkerheten i MTP ska utformas och hanteras.
  - En revidering av PDL, så att den harmoniserar med ny EU-förordning om MTP och PSL.

- På den internationella arenan initiera ett aktivt, långsiktigt förändringsarbete genom att driva de ståndpunkter och frågeställningar som rapporten berör. Detta kan ske via engagemang inom standardiseringsarbete, organisationer inom EU och internationella seminarier och liknande fora. Som exempel kan nämnas att Mats Ohlson, Läkemedelsverket, efterlyste en engelskspråkig version av vår första rapport som LV kunde sprida inom EU. LfMT:s styrelse bör bjuda in Läkemedelsverket till samtal för att ta fram en strategi i syfte att få upp problematiken på dagordningen hos tillsynsmyndigheterna inom EU.

LfMT bör även belysa frågan om ”Automatgenererad information och beslut” från MTP (t. ex. datortolkning av EKG) angående:

- Dess definition.
- Hur den upprättas.
- Hur dess autenticitet avgörs.
- Hur den ”Fastställs” och blir en ”Allmän handling”. Enligt våra minnesanteckningar från mötet med SOS och IVO, så är den automatgenererade informationen att jämställas med en ”minnesanteckning”, som omgående är färdig att tas i bruk och därmed anses vara ”upprättad” och därmed utgör en ”allmän handling”**.**
- Hur och när den får gallras.
- Urval och överföring av information från MTP till patientens journal.
- Uthopp från journalsystem till ”Automatgenererad information” lagrad i MTP.

Molnlagring

Vi har i denna rapport avsiktligt förbigått problematiken och frågeställningarna kring molnlagring av medicinska data, trots att den för tillfället utgör en av de ”hetaste” trenderna inom medicinsk informationshantering.

Arbetsgruppen anser emellertid att detta komplexa område är så pass omfattande att det utgör underlag för en egen utredning och att det skulle leda för långt att fördjupa sig i området inom ramen för denna rapport.

Avsnitt III:

Referenser

- SOSFS 2008:1. Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården
- LVFS 2003:11 Läkemedelsverkets föreskrifter om medicintekniska produkter;
- SS-ISO/IEC 27001 Ledningssystem för informationssäkerhet – Krav
- SS-ISO/IEC 27002 Riktlinjer för styrning av informationssäkerhet
- SS-ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27005 Information Security Risk Management
- Grimes S, Medical device security. PMID: 17271046 [PubMed].
- Fragopoulos A, Security Framework for Pervasive Healthcare Architectures Utilizing MPEG-21 IPMP Components. MID: 19132095 [PubMed].
- Guo R, An efficient and secure certificateless authentication protocol for healthcare system on wireless medical sensor networks. PMID: 23710147 [PubMed].
- Croll PR, Privacy with emergency medical information used in first response. PMID: 22797012 [PubMed].
- Kavoussi SC, HIPAA for physicians in the information age. PMID: 25195309 [PubMed]
- Cucoranu IC, Privacy and security of patient data in the pathology laboratory. PMID: 23599904 [PubMed]
- Calvillo J, Empowering citizens with access control mechanisms to their personal health resources. PMID: 17271046 [PubMed].
- Fernández-Alemán JL, Security and privacy in electronic health records: a systematic literature review.