Examensarbete

HÖGSKOLAN I SKÖVDE

PRIVACY BY DESIGN
Inbyggd integritet i patientjournaler

Examensarbete inom huvudområdet Datalogi
Grundnivå 15 högskolepoäng
Vårtermin 2013

Carl Simmingsköld

Handledare: Birgitta Lindström
Examinator: Rose-Mharie Åhlfeldt

Sammanfattning

I dagens hälso- och sjukvård behandlas patientuppgifter elektroniskt i patientjournalsystem. Uppgifterna ska behandlas med högsta möjliga säkerhetsåtgärder eftersom de innehåller känslig information om patienter. Patientuppgifterna behöver dock alltid vara tillgängliga för att vårdgivarna ska kunna ge bästa tänkbara vård. På grund av att hanteringen av patientinformation är kritisk, måste IT-systemen följa regler och upprätthålla en hög integritet. Privacy by Design (PbD) är tänkt att adressera problemet genom att integritetsaspekten får stå i fokus genom IT-systemets hela livscykel. PbD beskriver hur system ska vara, exempelvis att inte mer information än det som verkligen behövs ska samlas in, och att ge registrerade i IT-system insyn om vad som finns sparat om dem. Studien har analyserat på vilket sätt principerna och ramverket PbD används i patientjournalsystem för att skydda patientens integritet. Resultatet visar att det finns stora brister för att skydda patientens integritet framförallt genom avsaknad på kryptering i databaser och intern nätverkstrafik. Användarna kan dessutom tillgodose sig med mer information än de behöver och det finns dåligt med begränsningar för vad som kan skrivas in i patientjournalerna.

Nyckelord: Privacy by design, inbyggd integritet, personlig integritet, informationssäkerhet, e-hälsa

Innehållsförteckning

1 Introduktion

I dagens samhälle lagras, sprids och bearbetas mer information än någonsin tidigare. För att informationen ska vara säker krävs flera olika insatser. Informationssäkerhetsarbetet är ett komplext område och ses ofta enbart som en kostnad för att upprätthålla säkerhet.

Inom hälso- och sjukvården behandlas många uppgifter som är känsliga. Dessa uppgifter bör behandlas med högsta möjliga säkerhetsåtgärder för att patienten ska få bästa tänkbara vård. För att patienterna ska få bästa tänkbara vård måste rätt information vara tillgänglig vid rätt tidpunkt (Åhlfeldt & Söderström, 2007). Informationen måste vara korrekt för att undvika felbehandlingar. Patienter måste även känna tillit till systemen, annars finns risken att de utelämnar uppgifter som behövs för vården (Fetter, 2009). På grund av att hanteringen av patientinformation är kritisk måste IT-systemen följa regler och upprätthålla en hög integritet. Integriteten kompliceras av att informationen hanteras av flera system och vårdgivare, ökad tillgänglighet mellan vårdgivare ökar risken för att information läcker ut.

Fetter (2009) skriver att den största utmaningen med elektroniska patientjournaler är att implementera tillräckliga säkerhetsåtgärder. Bland dessa är autentisering, auktorisering, övervakning av tillträde, skydd av lagrad data, skydd av datakommunikation, skydd av data på bärbara datorer och bärbara enheter.

En tidigare studie (Socialstyrelsen, 2004) visar att det inte är sambandet mellan respektive vårdpersonal och patient som styr behörigheten utan yrket vårdpersonalen har. Varje yrkesgrupp har en generell användarprofil som är centralt fastställd. Utifrån de svar som lämnades till studien framkom det inte att det fanns regler och villkor hur användarna fick använda de tilldelade behörigheterna. Studier visar (Åhlfeldt & Söderström, 2007) att de största bristerna ligger i den administrativa säkerheten, och att en helhetslösning som inkluderar integritetsfrågor behövs. Privacy by Design (PbD) är tänkt att adressera problemet genom att integritetsaspeken får stå i fokus genom IT-systemets hela livscykel. PbD beskriver hur system ska vara, exempelvis att inte mer information än det som verkligen behövs ska samlas in, och att ge registrerade i IT-system insyn om vad som finns sparat om dem. Studien kommer analysera hur väl PbD i praktiken överensstämmer med hur PbD teoretiskt beskriver hur IT-system ska vara. Vilka hinder det finns, och om det ens är möjligt att anamma PbD fullt ut i hälso- och sjukvården. Målet i studien är därför att undersöka hur, och till vilken grad principerna och ramverket PbD används på patientjournalsystem för att skydda patientens integritet.

Två patientjournalsystem inom hälso- och sjukvården kommer att analyseras. Anledningen till att just patientjournalsystem analyseras beror på att de innehåller känsliga personuppgifter, och att det då krävs extra krav på hantering av personuppgifter. Arbetet fokuserar på en analys avseende PbD av själva patientjournalsystemen med kringliggande rutiner, samt även hur implementeringen av integritetsåtgärder av patientjournalsystemen har genomförts. Patientjournalsystemet i ett av landstingen är integrerat med en applikation som tillåter medborgare direktåtkomst av sin journal på nätet. Applikationen lagrar ingen patientdata men läser av från det existerande patientjournalsystemet. Även denna applikation ska analyseras.

2 Bakgrund

Under denna rubrik kommer koncept inom informationssäkerhet att beskrivas för att öka förståelsen för läsaren. PbD förklaras mer ingående med de sju grundläggande principerna. Vilket sätt patientdata får hanteras, och vilken information som får finnas lagrade inom hälso- och sjukvården. Problem som finns med avseende på integritetsaspekter inom hälso- och sjukvården beskrivs. Avsnittet avslutas med relaterade arbeten till PbD.

2.1 Informationssäkerhet

Informationssäkerhet handlar om förmågan att säkerställa informationstillgångar med avseende på egenskaperna tillgänglighet, riktighet och sekretess. Även spårbarhet är vanligt förekommande inom informationssäkerhet.

Swedish Standard Institute (2003) definierar de följande egenskaperna:

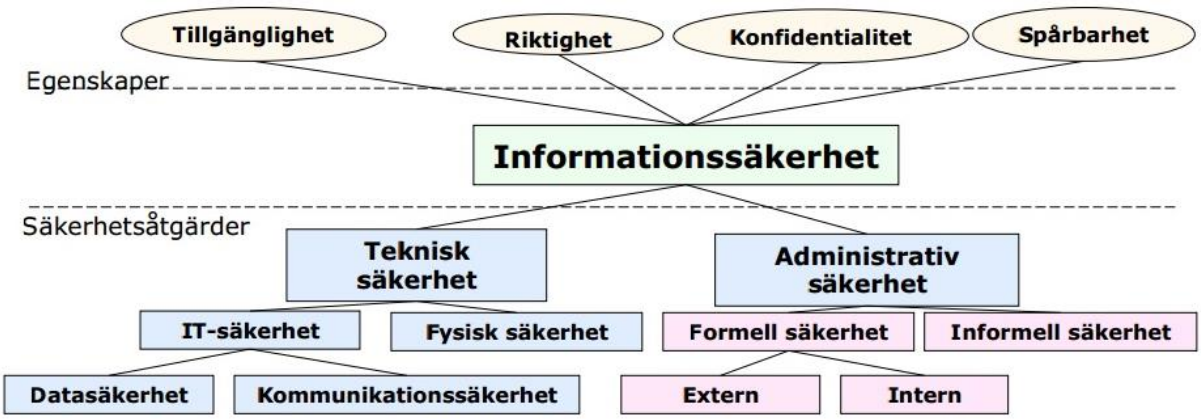
• Tillgänglighet: ”*Möjligheten att utnyttja informationstillgångar efter behov i förväntad utsträckning och inom önskad tid*”.

• Riktighet: ”*Egenskap att information inte obehörigen, av misstag eller på grund av funktionsstörning har förändrats*”.

• Sekretess: ”*Avsikten att innehållet i ett informationsobjekt inte får göras tillgängligt eller avslöjas för obehöriga*”.

• Spårbarhet: ”*Möjlighet att entydigt kunna härleda utförda aktiviteter i systemet till en identifierad användare*”.

För att de fyra egenskaperna ska uppnås, och för att kunna angripa riskerna på ett effektivt sätt, behöver man ofta dela upp informationssäkerhetsarbetet i olika områden. De två huvudområdena kan delas upp i administrativ säkerhet och teknisk säkerhet. Syftet med administrativ säkerhet är att skydda informationstillgångar genom riskanalys, införa strategier och policys, utbildning med mera. Det finns även formell administrativ säkerhet vilket syftar på att lagar, regler och andra bestämmelser måste följas. Tekniska säkerhetsåtgärder kan delas upp i IT-säkerhet och fysisk säkerhet. IT-säkerhet handlar om kommunikationssäkerhet och datasäkerhet som kan skyddas genom exempelvis brandväggar, autentisering och kryptering. Fysisk säkerhet handlar om hur utrustning skyddas mot fysiska hot genom exempelvis skalskydd, strategisk placering utav utrustning och larm.



Figur 1 Informationssäkerhetsmodellen (Åhlfeldt & Söderström, 2007).

Kommer en patient till sjukhuset och är i behov av akut vård, måste patientjournalen vara tillgänglig för att vårdgivaren ska kunna ge bästa tänkbara vård. Vårdgivaren måste ha tillgång till patientjournalen för att se om patienten lider av några sjukdomar sedan tidigare för att veta hur patienten ska behandlas. Brist på information får inte leda till felbehandling genom att vårdgivaren exempelvis överdoserar medicin eftersom de inte har tillgång till information om vilka mediciner patienten använder. Patientdata måste även finnas tillgängliga från andra vårdgivare där patienten har behandlats innan. Det finns flera åtgärder för att minimera risken att patientdata inte finns tillgänglig när vårdgivaren behöver den, dock måste en avvägning ske för att inte sekretessen ska äventyras. I nästa avsnitt beskrivs PbD som är tänkt att adressera problemet genom att integritetsaspekten får stå i fokus genom IT-systems hela livscykel.

2.2 Privacy by design

PbD går ut på att grundläggande principer påverkar integriteten i IT-system under hela dess livscykel genom förstudie, design, utveckling och avveckling. PbD är inbäddat i designen och arkitekturen av systemet istället för att vara något som läggs till i efterhand. Integritet blir integrerat som en del i systemet, utan att minska funktionalitet. Redan innan den första informationen samlas in är integritet inbäddat, och ända till avvecklingen av IT-system där det säkerställs att all data förstörs när systemen ska tas ur bruk. Några av dessa grundläggande principer är exempelvis transparens, vilket syftar på att ge individer som är registrerade i systemen insyn i vad som finns sparat om dem, att inte mer information än det som behövs ska samlas in, och att arbetet kring IT-systemen ska göras förebyggande istället för när incidenter sker.

PbD gör att IT-system slipper att hamna i fallgropar som blir komplicerade att åtgärda i efterhand, det kan bli både dyrt och svårt att följa lagar med hänsyn till integritetsaspekter. PbD är ett begrepp som utvecklades av Dr. Ann Cavoukian på 90-talet. På den tiden var det mindre populärt att bädda in integritet i designen med teknologi. Men sedan dess har saker och ting förändrats mycket. Tillvägagångsättet PbD är idag mycket populärt (Cavoukian, 2011). Principerna i PbD har blivit anammat av bland annat EU och U.S. Federal Trade Commission. De har även antagits som en internationell standard av flera dataskyddsmyndigheter (Fineberg & Jeselon, 2011). Datainspektionen i Sverige har släppt ett informationsblad om PbD, eller inbyggd integritet som det heter på svenska. Informationsbladet ger en vägledning i hur arbetet med PbD kan utformas

(Datainspektionen, 2012). Principerna i PbD kan tillämpas på alla typer av personlig information, men bör tillämpas med extra kraft på känslig data som innehåller ekonomiska och medicinska uppgifter. Cavoukian (2011) beskriver de sju grundläggande principerna i PbD:

- "*Proactive not Reactive; Preventative not Remedial*": Vilket innebär att arbetet sker förebyggande istället för att agera när incidenter händer.
- "*Privacy as the Default Setting*": PbD syftar till att ge högsta tänkbara integritet genom att personuppgifter automatiskt skyddas i IT-system. Den enskilde individen behöver inte göra något för att skydda sin integritet – det är inbyggt i systemet, som standard.
- "*Privacy Embedded into Design*": PbD ska vara inbäddat i designen och arkitekturen av systemet istället för att vara något man lägger till i efterhand. Integritet blir integrerat som en del i systemet, utan att minska funktionalitet.
- "*Full Functionality — Positive-Sum, not Zero-Sum*": PbD syftar till att alla intressen ska vara positiva och vara i win-win situationer där inga onödiga kompromisser görs.
- "*End-to-End Security — Full Lifecycle Protection*": Integritet är inbäddat i systemet under hela livscykeln. Redan innan den första informationen samlas in är integritet inbäddat och PbD säkerställer att all data förstörs när IT-systemen ska tas ur bruk.
- "*Visibility and Transparency — Keep it Open*": Syftar till att alla intressenter ska kunna verifiera att uppställda löften och mål uppnås. Delar och funktioner förblir synliga och transparanta för användare och leverantörer.
- "*Respect for User Privacy — Keep it User-Centric*": PbD kräver att arkitekter och operatörer ska tänka på den enskilda individens intressen först och främst genom att erbjuda stark integritet som standard och användarvänliga funktioner.

2.2.1 PbD – PIA

A Foundational Framework for a PbD – PIA (Privacy Impact Assessment) är ett grundläggande ramverk för PbD.

Det är en utmaning att implementera den teoretiska filosofin PbD i praktiken till organisatoriska lösningar, det vill säga hur man får PbD att fungera i driften av IT-system. PbD – PIA har därför skapats som ett praktiskt hjälpmedel till organisationer för att styra och informera i utformingen av IT-system. Ramverket ska säkerställa att integritet och funktionalitet byggs in från början (Fineberg & Jeselon, 2011). Lokala lagar och bestämmelser måste dock alltid kontrolleras eftersom ramverket inte kan ersätta dem (Fineberg & Jeselon, 2011).

2.3 Personuppgiftslagen

Under denna rubrik kommer Personuppgiftslagen (PUL) att beskrivas eftersom patientjournalsystemen innehåller personuppgifter. Det krävs då att Personuppgiftslagen följs.

I personuppgiftslagen (SHS 1998: 204) står det att den som är personuppgiftsansvarig är:

"Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter"

Ansvariga för IT-systemen ska se till att systemen är utformade på ett sådant sätt som inte medför integritetsrisker. Personuppgiftslagen är till för att skydda personer mot att deras personliga integritet kränks. Lagen kräver att uppgifter skyddas när de samlas in, registreras, lagras, bearbetas, sprids med mera. Det finns regler i personuppgiftslagen som talar om hur uppgifterna får behandlas. Totalt består personuppgiftslagen av 53 paragrafer. Det finns dock undantag i lagen som gör att personuppgifter som hanteras på ett ostrukturerat sätt har en förenklad reglering. Ostrukturerade material innebär att personuppgifter förekommer i löpande text, exempelvis i Word dokument eller via email. Strukturerat material innebär att personuppgifterna förekommer i databaser och liknande. Dessa har mycket striktare villkor på sig än det ostrukturerade materialet (SFS 1998: 204). Patientdata är klassad som känslig information, vilket betyder att den är förbjudet att behandla. Det finns dock undantag från förbudet mot behandling av känsliga personuppgifter.

I personuppgiftslagen (SHS 1998: 204) står det att:

*”**18 §** Känsliga personuppgifter får behandlas för hälso- och sjukvårdsändamål, om behandlingen är nödvändig för*
a) förebyggande hälso- och sjukvård,
b) medicinska diagnoser,
c) vård eller behandling, eller
d) administration av hälso- och sjukvård”.

Vårdguiden (2012) skriver att följande uppgifter kan registreras:

- ”*Personuppgifter, till exempel namn, personnummer, adress och e-postadress*”.
- ”*Besök på vårdcentraler och sjukhusmottagningar*”.
- ”*Besök på tandvårdskliniker och hjälpmedelscentraler*”.
- ”*Inskrivningar för sjukhusvård*”.
- ”*Undersökningar, operationer och andra åtgärder*”.
- ”*Diagnoser*”.
- ”*Resor i samband med vård*”.
- ”*Ekonomiska transaktioner*”.

2.4 Patientdatalagen

Patientdatalagen infördes 2008 och ersatte patientjournallagen och vårdregisterlagen. När patientdata hanteras av vårdgivare inom hälso- och sjukvården tillämpas patientdatalagen. I lagen finns bestämmelser om skyldigheter för att föra patientjournal (SFS 2008: 255). Varje gång en patient besöker hälso- och sjukvården registreras uppgifter om patienten. Detta är ett krav enligt patientdatalagen för att patienter ska få en så god vård som möjligt (Vårdguiden, 2012). Patientdatalagen beskriver vem som är skyldig att föra journalhandlingar och vad patientjournalen ska innehålla. Den innehåller även bestämmelser om kvalitetsregister inom sjukvården samt bestämmelser om sammanhållen journalföring, som innebär att vårdgivare under vissa omständigheter kan göra patientjournaler tillgänglig för andra vårdgivare.

2.5 Patientjournaler

Förutom personuppgifter kan patientjournalen innehålla diagnoser, behandlingar, tidigare vård och planerad behandling, samt vem som antecknat vad och vid vilken tidpunkt. I dag använder fler och fler samma journalsystem vilket innebär att patientdata kan delas mellan olika vårdgivare. Det är vårdgivarens skyldighet att informera patienten om vad det innebär. När information ska hämtas ifrån en annan vårdgivare måste vårdgivaren hämta in samtycke från patienten (Vårdguiden, 2012).

2.5.1 Elektroniska patientjournaler

Begreppet elektroniska patientjournaler definieras som en samling av hälsoinformation, som lagras elektroniskt, om patienter. På engelska; Electronic health record (EHR). Elektroniska patientjournaler är främst till för att samla in information som idag finns i pappersform och elektroniskt för att förbättra kvaliteten i hälso- och sjukvården (Gunter & Terry, 2005).

Många experter och kliniker är oroliga över hur patienters personliga integritet påverkas av att elektroniska patientjournaler implementeras. IT-systemen gör att tredje man, som exempelvis leverantörer av patientjournalsystem, får tillgång till patienters uppgifter (Fetter, 2009). Den största utmaningen med elektroniska patientjournaler är att implementera tillräckliga säkerhetsåtgärder. Bland dessa är autentisering, auktorisering, övervakning av tillträde, skydd av lagrad data, skydd av datakommunikation, skydd av data på bärbara datorer och bärbara enheter. (Fetter, 2009).

En tidigare studie (Socialstyrelsen, 2004) visar att det inte är sambandet mellan respektive vårdpersonal och patient som styr behörigheten, utan yrket vårdpersonalen har. Varje yrkesgrupp har en generell användarprofil som är centralt fastställd. Utifrån de svar som lämnades till studien framkom det inte att det fanns regler och villkor om hur användarna fick använda de tilldelade behörigheterna.

Känsliga uppgifter som läcker ut kan leda till att diskriminering sker i exempelvis arbetslivet. Patienter som känner att det finns säkerhetsbrister inom hälso- och sjukvården kan välja att avstå, eller inte ange all information som är nödvändig för deras behandling, eftersom de är rädda för att informationen ska komma ut (Fetter, 2009).

I en fallstudie (Åhlfeldt & Söderström, 2007) framkommer flera brister inom hälso- och sjukvården när information ska delas mellan flera vårdgivare. Det finns otillräckliga verktyg för logghantering, brister i autentisering och auktorisering. Patientinformation kan förloras på grund av dåliga backuprutiner. De intervjuade personerna anser genomgående att administrativ säkerhet är det största problemet inom hälso- och sjukvården. Tre av fem svarade att det är brister i tillgänglighet som är den största problemkällan. De intervjuade blev frågade om vilka tänkbara framtida brister som skulle kunna finnas inom hälso- och sjukvården även om tillgängligheten förbättrades. Återigen dominerade de administrativa säkerhetsproblemen.

2.6 Relaterade arbeten

Van Lieshout, Kool, Van Schoonhoven och de Jonge (2011) skriver att det finns relativt lite forskning angående hur väl fungerande PbD är på att säkra system. De har genom att göra begreppsanalys, intervjuer och teknisk demonstration kommit fram till att PbD kan säkra system utan att funktioner blir lidande. Dock är implementeringen av PbD inte helt lätt då

projekt kan ställas inför flera svårigheter som ekonomi, äldre system och brist på förtroende från användarna av systemen.

Transparens på personliga uppgifter som bearbetas är en viktig princip för den enskilda individen. Transparens är ett viktigt medel för att förbättra förtroende till användaren. Forskare inom PRIME projektet skriver att förtroendet för system kan förbättras om de är transparenta och tydliga så att användarna känner kontroll (Fischer-Hübner, 2011). Transparens och synlighet är en av de grundläggande principerna i PbD och syftar till att de registrerade ska ha insyn i systemen. Att system är transparenta menas i fallet med patientjournalsystem, att patienterna exempelvis ska ha tillgång till att se vilken information som är sparad om dem i patientjournalsystemen, vem som lagt in informationen, och vem som läst informationen.

3 Problem

Integritet är extra viktig i hälso- och sjukvården eftersom känslig information hanteras. För att patienter ska få bästa vård krävs det att rätt information finns tillgänglig vid rätt tillfälle, och att informationen är korrekt för att undvika felbehandlingar.

Tillgängligheten i patientjournalsystem är extra kritisk när patienter kommer till sjukhus och är i behov av akutvård. Vårdgivaren måste då ha tillgång till patientdata som beskriver tidigare diagnoser och eventuell medicinering. Om en patient kommer in och t.ex. har väldigt svårt att andas, kan vårdgivaren se i patientjournalsystemet om patienten är allergisk mot något, och vet då vilken medicin de ska ge. Kommer det in en medvetslös patient som inte är kontaktbar och inte kan svara på frågor om tidigare sjukdomar, blir det svårt för vårdgivaren att veta vad som hänt om patientjournalsystemet inte fungerar. Patientdata måste även finnas tillgängliga från andra vårdgivare där patienten har behandlats innan. Brist på tillgänglighet får inte leda till felbehandling som exempelvis överdosering av mediciner.

När tillgängligheten förbättras måste dock alltid en avvägning ske mot sekretess eftersom det innebär en större risk att information görs tillgänglig för obehöriga. Brist på patienttrygghet kan leda till att patienterna utelämnar känslig information som behövs för vårda patienten. Det finns även lagar som styr hur känsliga uppgifter får behandlas. På grund av att hantering av patientinformation är kritisk, måste även IT-systemen följa regler och upprätthålla en hög integritet. Integriteten kompliceras av att informationen hanteras av flera system och vårdgivare, ökad tillgänglighet mellan vårdgivare ökar risken för att information läcker ut. Hantering av patientinformation mellan flera vårdgivare är dock nödvändig för att vårdgivare ska ha tillgång till nödvändig information för att vårda patienterna.

Studier visar (Åhlfeldt & Söderström, 2007) också att de största bristerna ligger i just den administrativa säkerheten. PbD är tänkt att adressera problemet genom att integritetsaspeken får stå i fokus genom IT-systemets hela livscykel. Det är därför önskvärt att PbD anammas för IT-system inom hälso- och sjukvården.

PbD beskriver hur system ska vara, exempelvis att inte mer information än det som verkligen behövs ska samlas in och att ge registrerade i system insyn om vad som finns sparat om dem. Studien kommer att analysera hur väl PbD i praktiken överensstämmer med hur PbD teoretiskt beskriver hur IT-system ska vara. Vilka hinder det finns och om det ens är möjligt att anamma PbD fullt ut i hälso- och sjukvården. Målet i studien är därför att undersöka hur, och till vilken grad, principerna och ramverket i PbD används på patientjournalsystem för att skydda patientens integritet.

3.1 Problemprecisering

Målet med studien är att besvara följande fråga:

På vilket sätt används principerna och ramverket PbD i patientjournalsystem för att skydda patientens integritet?

För att förtydliga målet delades frågan upp i fem områden.

- Minimering av personuppgifter som samlas in i IT-system. Vilket syftar på vad landstingen och patientjournalföretagen gör för att minska antalet personuppgifter i IT-systemen.

- Åtkomst i IT-system. Hur landstingen och patientjournalföretagen arbetar med utformning av IT-systemen så enbart användare som arbetar med informationen ska ha åtkomst till den.

- Skydda uppgifterna. Hur information skyddas med säkerhetsfunktioner som autentisering, kryptering och fysisk säkerhet.

- Låt IT-systemen styra användaren rätt. Hur användarvänliga IT-systemen är och om de styr användaren i rätt riktning för att integritetssäkra information.

- Transparens. Hur de registrerade har insyn i IT-systemen, i det är fallet hur patienter kan se vad som finns lagrat om dem i patientjournalsystemen.

3.2 Avgränsning

Två patientjournalsystem inom hälso- och sjukvården kommer att analyseras. Anledningen till att just patientjournalsystem analyseras beror på att de innehåller känsliga personuppgifter och att det då krävs extra krav på hantering av personuppgifter. Arbetet fokuserar på en analys avseende PbD av själva patientjournalsystemen med kringliggande rutiner, samt även hur implementeringen av integritetsåtgärder av patientjournalsystemen har genomförts. Patientjournalsystemet i ett av landstingen är integrerat med en applikation som tillåter medborgare direktåtkomst av sin journal på nätet. Applikationen lagrar ingen patientdata, men läser av från det existerande patientjournalsystemet. Även denna applikation ska analyseras.

4 Metod

Berndtsson, Hansson, Olsson och Lundell (2008) tar upp flera olika metoder och tekniker som är tänkbara att använda som angreppssätt till problemet. Några av de metoder som de tar upp i boken är litteraturstudie, intervju, fallstudie, enkäter, implementering och experiment. Reflektioner har gjorts på några av de tänkbara metoderna till problemet.

4.1 Litteraturstudie

Datainspektionens informationsblad (2013) och forskningsartiklar inom PbD har använts för att få en så stor förståelse som möjligt hur system ska utvecklas enligt PbD. Datainspektionens informationsblad och forskningsartiklarna har sedan använts för att formulera frågor som ska passa att ställas till personer som har en god insikt i hur patientjournalsystemen fungerar. Svaren har sedan analyserats mot forskning om PbD för att kontrollera hur IT-systemen i praktiken överensstämmer med PbD filosofin.

4.2 Intervjuer

Intervjuer kan göras på olika sätt. I en öppen intervju ska frågor ställas så att respondenten öppnar upp sig och ger berättande svar. Respondenten ska tillåtas att svara på frågan utifrån sina egna ord. Öppna intervjuer kan förhindra att ledande frågor ställs där det ibland bara går att svara ja eller nej. Nackdelen men öppna intervjuer är att de kan vara svåra att hantera för personer med lite erfarenhet (Berndtsson, Hansson, Olsson och Lundell, 2008). I en strukturerad intervju används förbestämda frågor. Frågor kan inte tas bort eller läggas till utifrån de svar intervjuaren får från respondenten. Frågorna är mer begränsade, vilket kan påverka respondentens motivation negativt så att fullständiga svar inte ges. Strukturerade frågor är mer vanliga att använda i enkätundersökningar (Berndtsson, Hansson, Olsson och Lundell, 2008).

4.3 Enkätundersökning

Enkätundersökningar används oftast när ett relativt känt fenomen som det finns många personer som kan svara på. Nackdelen med enkätundersökningar är att komplicerade problem blir svåra att redogöra, eftersom det inte är någon tvåvägskommunikation mellan den som intervjuar och respondenten. Det är omöjligt att förtydliga svar (Berndtsson, Hansson, Olsson och Lundell, 2008). En annan nackdel är att respondenters motivation är låg. Det är i allmänhet svårt att få en hög svarsfrekvens. Det har sagts att genom enkätundersökning är det omöjligt att veta det verkliga intrycket ifrån respondenterna (Berndtsson, Hansson, Olsson och Lundell, 2008).

Det är flera olika orsaker till att enkätundersökningar har valts bort som metod till arbetet. Dels för att det är svårt att redogöra för komplicerade problem med en enkätundersökning, dels för att följdfrågor inte kan ställas, och dels för att förtydligande svar inte kan ges om det är något som är oklart.

4.4 Val av metod

Metoden som valts för att analysera journalsystemen utifrån PbD är öppna intervjuer med systemutvecklare och personer som har mycket god insikt i systemen. Anledningen till att

öppna intervjuer används är för att svaren blir mer utförliga, och för att eventuella frågor som uppstår av svaren kan besvaras direkt. Förtydligande svar kan ges om något är oklart.

5 Genomförande

Ur säkerhetssynpunkt kommer landstingen att anonymiseras och presenteras som Landsting A och Landsting B. Rollen som den intervjuade respondenten har kommer dock att presenteras.

I ett tidigt skede av studien var tanken att intervjua informationssäkerhetsansvariga och kravställare inom landstingen, men även utvecklare till patientjournalsystemen och applikationen för att nå patientjournaler på nätet. Intervjuförfrågan skickades via mail till nämnda personer som var svåra att få kontakt med. Förfrågan för intervju skickades därför till flera personer med olika roller för att hitta personer som kunde hjälpa till att svara på frågorna. Slutligen intervjuades totalt sex personer. På Landsting A intervjuades rollerna IT-säkerhetsansvarig, personuppgiftsombud och kravanalytiker på företaget som utvecklar patientjournalsystemet. På Landsting B intervjuades informationssäkerhetsansvarig, IT-strateg och systemutvecklare på företaget som utvecklar applikationen för att nå patientjournalen på nätet. Personer som ställt upp på intervju presenteras mer under resultatdelen tillsammans med svaren på frågorna. Varje intervju tog mellan 15-45 minuter. Anledningen till att informationssäkerhetsansvarig valdes för intervju är för att de har en övergripande syn över säkerheten, men även för att de har ett övergripande ansvar inom organisationen för integritetsfrågor. Kravställare eftersom de ska se till att ställa de krav som behövs på system för att verksamhetens mål ska uppfyllas. Systemutvecklare skulle intervjuas eftersom de har inblick i hur systemen tekniskt är utformade, och vilka säkerhetsfunktioner som finns implementerade i journalsystemen.

De olika frågekategorierna är inte uppdelade efter de sju grundläggande principerna inom PbD, utan datainspektionens informationsblad (2013) har huvudsakligen används när frågorna utformades, och studien har därför valt följa deras checklista. Anledningen till att datainspektionens informationsblad används är för att det är utformat av en svensk myndighet och studien gör en analys av patientjournalsystem i Sverige. PbD - PIA ramverket säkerställer inte att lokala lagar följs, utan ramverket måste anpassas efter lokala lagar och bestämmelser (Fineberg & Jeselon, 2011). Det är därför önskvärt att följa en svensk myndighets checklista för PbD. För att undvika att ställa ledande frågor har de flesta frågor formulerats så att respondenten ska förklara HUR saker är i deras IT-system istället för OM. Exempelvis ”*Hur är data på era backuper skyddade?*” Istället för att fråga OM deras backuper är krypterade och inlåsta. Upplägget på en HUR fråga ger oftast ett mer berättande svar från respondenten då de kan öppna sig för att diskutera viktiga problem (Berndtsson, Hansson, Olsson och Lundell, 2008).

När intervjuerna var färdiga skrevs en sammanfattning av svaren. Upprepningar och saker som var irrelevant för frågan sorterades bort. Sammanfattningen på frågorna skickades tillbaka till respondenterna för verifiering så att inte några svar hade missuppfattats, och för att få ett godkännande (Kravanalytiker (A), Personuppgiftsombud (A), Systemutvecklare (B) har svarat på mailet). Respondenterna frågades även om det var något som de ville tillägga eller ta bort.

Sammanfattningen av svaren finns att läsa i resultatavsnittet. Under analysavsnittet beskrivs sedan hur väl patientjournalsystemen överensstämmer med hur PbD beskriver att IT-system ska vara.

Studien ingår som en delstudie i forskningsprojektet Deployment of online medical records and eHealth sevices (DOME) som har som mål att bygga upp kunskap om införandet och användning av e-hälsotjänster[1]. De två landsting som analyserats i denna uppsats använder olika patientjournalsystem utvecklade av olika företag. I ett av landstingen erbjuds även medborgare att nå sin journal direkt på nätet.

[1] Mer information om DOME finns på följande sida:
http://www.it.uu.se/research/hci/dome

6 Resultat

Nedan presenteras svaren från personerna som har blivit intervjuade. Frågorna som ställdes till respondenterna finns i Bilaga A.

6.1 Presentation av respondenter

IT-säkerhetsansvarig (A): IT-säkerhetsansvarig inom Landsting A.
Anställd sen maj 2007 och hade först en delad roll. Övergick sommaren 2008 helt till tjänsten som IT-säkerhetetsansvarig. Har deltagit i utbildningar sedan 1990, har hela tiden sedan dess byggt på med kurser och utbildningar ifrån IT-leverantörer, försvarshögskolan, högskolor och universitet.

Kravanalytiker (A): Respondenten jobbar främst med kravinsamling och kravspecifikation och saknar teknikerbakgrund. Respondenten hänvisar därför dessa frågor till mer tekniskt kunniga medarbetare. Respondenten har jobbat på företaget sedan september 2012 och är ganska ny på företaget men inte ny i sin roll, utan har jobbat med liknande arbetsuppgifter på ett konkurrerande journalsystemsföretag. Har under hela sin yrkesverksamma tid läst parallellt på universitet, men har ingen examen. Har läst kurser på 25 % -150 %, beroende på arbetsbelastning, inom området vårdmanagement, IT-projektledning, hälso- och sjukvårdsadministration, hälso- och sjukvårdsjuridik och verksamhetsuppföljning. Respondenten har ingen vårdbakgrund utan har sin tyngdpunkt inom vårdadministration. Denna bakgrund är respondenten ganska ensam om på företaget, där de allra flesta har en bakgrund som sjuksköterska, sekreterare, arbetsterapeut eller liknande.

Personuppgiftsombud (A): Respondenten är säkerhetssamordnare/personuppgiftsombud på ett sjukhus inom Landsting A, där respondenten varit anställd en längre tid. Respondenten har högskoleutbildning.

Informationssäkerhetsansvarig (B): Respondenten har haft rollen informationssäkerhetsansvarig i ett och ett halvt år på Landsting B. Jobbat tio år totalt inom landstinget. Respondenten har utbildning inom matte och data på universitet och genomfört utbildningar internt.

IT-strateg (B): Respondenten är projektledare för applikationen som tillåter medborgare direktåtkomst av sin journal på nätet. Därutöver är respondenten IT-strateg. Har tidigare arbetat med patientjournalsystemet som systemadministratör och utbildare. Kan därför svara på frågor om både applikationen och patientjournalsystemet. Varit anställd i landstinget sedan 2001 och haft nuvarande roll sedan 2012. Utbildad inom vården.

Systemutvecklare (B): Respondenten har rollen som systemutvecklare i ett företag som jobbar med e-hälsotjänster för invånare. De har inte byggt ett patientjournalsystem, utan en applikation som läser information från ett existerande patientjournalsystem. Respondenten har också jobbat med kravhantering och har varit anställd på företaget sedan december 2011 samt är utbildad systemutvecklare.

6.2 Minimering av personuppgifter som samlas in i IT-system

Under detta avsnitt presenteras resultatet från frågorna angående hur de minimerar personuppgifter som samlas in i IT-systemen.

6.2.1 Minimera uppgifter som samlas in

Kravanalytiker (A): Respondenten berättar ur sitt perspektiv som kravanalytiker hur de gör för att minimera uppgifter som samlas in. Varje gång innan de gör en ny funktion, eller ändrar en existerande funktion, finns det ett behov som föreligger. De börjar alltid med en behovsanalys. I behovsanalysen hjälper kravanalytikerna till att selektera ut vad det faktiska behovet är, så de inte samlar på sig exempelvis personuppgifter som inte behövs i sammanhanget. Funktionen specificeras alltid med utgångspunkt till behovet. Ofta vill kunderna samla på sig för mycket information. Det kan vara personuppgifter och annat som de vill kunna samla in om man skulle behöva det i framtiden. Det de försöker sålla bort i det här fallet är onödig lagring av personuppgifter. Kravanalytikern och kollegorna är ”grindvakter” angående vilka personuppgifter som ska lagras och inte lagras.

Att rätta till saker i produkterna är otroligt kostsamt så de försöker sortera bort så mycket som möjligt. Om man tittar på trenden både inom deras företag liksom andra företag, så är tendensen att mer och mer resurser läggs på krav. Det har kommit de senaste åren. Respondenten har jobbat med detta i fem år och de första åren lades knappt någon tid på det alls.

Det inte är upp till dem som leverantör, eller för all del kunden att bestämma vad som är extra känsliga personuppgifter. Det är patienten som bedömer vad om är känsligt eller inte. Sedan kan vissa uppgifter vara känsliga i vissa sammanhang utan att patienten ska ha någon åsikt om det, exempelvis när patienten ska ha skyddade uppgifter. I dessa fall har deras kunder i de flesta fall rutiner. Det är inget systemmässigt som hanterar extra känsliga uppgifter, utan där kommer patientdatalagen in och gör det möjligt att spärra uppgifter som patienterna tycker är känsliga, men journalsystemsleverantören gör inte den bedömningen.

Som leverantör görs mycket arbete i kravspecifikationens framställande för att se till att datainsamlingen är lämplig och relevant. Dessutom finns ett personuppgiftsansvar och det ligger på vårdgivarna. Den löpande kontrollen, d.v.s. att om behovsbilden förändras, är något som kunderna först känner till. Om behovet av en viss uppgift har förändrats har de sämre kontroll. Där litar de på att kunderna tar kontakt med dem om exempelvis en ändring av systemet behövs, eller att en uppgift ska tas bort. Respondenten tror att uppföljningen hos deras kunder är ganska dålig. Respondenten är tveksam till om den fortföljande uppföljningen, om man fortfarande behöver något görs överhuvudtaget. Under de fem år respondenten jobbat har respondenten inte tagit emot speciellt många önskemål om att man vill ta bort något p.g.a. ändrade behovsbilder. Även om man haft anledning till det. Detta ser respondenten som ganska allvarligt.

Personuppgiftsombud (A): Genom återkommande revisioner minimeras mängden personuppgifter som samlas in. Personuppgifter ska inte sparas längre än vad som är nödvändigt. De följer regionens dokumenthanteringsplan för vilka uppgifter som får samlas in.

Patientjournal ska föras enligt lagen för varje individ. Till det tillkommer säkerhetsaspekter med medicinsk spårbarhet. Alla register som innehåller personuppgifter ska anmälas till personuppgiftsombudet där även en säkerhetsgranskning sker.

Det finns alltid personuppgifter som kan vara extra känsliga, personuppgifter inom hälso- och sjukvården klassas enligt personuppgiftslagen som känsliga personuppgifter.

Genom revisioner kontrolleras datainsamlingen periodiskt. Lagen används som bakgrund för vad som får samlas in för det mesta då datafångsten är journalföring. De har en spårbarhet i systemet där de kan se vem som gjort vad och när.

Informationssäkerhetsansvarig (B): Lagstiftning styr vilka uppgifter de måste föra in eftersom de har betydelse för vården. Egentligen kan man säga att dels är det lagstiftat och dels utbildar de personalen. Därefter görs kvalitetskontroller på det som skrivs in i patientjournalen. Sökord används för att se vilken typ av uppgifter som kan skrivas in. Patientuppgifter hanteras lika. Men skyddade personuppgifter hanteras annorlunda. Verksamhetscheferna gör kvalitetssäkringar på datainsamlingen för att säkerställa att den är lämplig och relevant, och inte överdrivet omfattande i förhållande till dess ändamål. De gör centralt inga kontroller för datainsamlingen.

IT-strateg (B): De arbetar utifrån sökordsmallar och sökord, vilket gör att det är många fasta val och många numeriska värden som fylls i. Respondenten kan inte svara på om alla personuppgifter hanteras likadant, eller om det är vissa som är extra känsliga och hanteras mer försiktigt, men det finns rutiner för att kolla upp om uppgifter är lämpliga och relevanta och inte överdrivet omfattande i förhållande till dess ändamål. Kvalitetssäkring bland annat.

Systemutvecklare (B): Applikationen företaget använder är en läsare som är integrerad med existerande patientjournalsystem, vilket innebär att de inte lagrar patientdata utan läser den enbart från patientjournalsystemet. Applikationen har dock en databas som lagrar förnamn, efternamn och personnummer som är kopplat till användaren. De samlar även in länstillhörighet, men det är inte kopplat till användaren i databasen, utan används för verksamhetsuppföljning för att samla in statistik för de som loggat in på systemet. Respondenten tillägger att de lagrar enbart de personuppgifter de absolut behöver.

6.2.2 Uppgifter för identifiering

IT-säkerhetsansvarig (A): Reservnummer används för att identifiera patienten. Genom reservnummer kan patienter inte identifieras direkt så numren fungerar som pseudonymer.

Kravanalytiker (A): Personnummer eller pseudonymer kan användas för identifiering. Det finns lagstiftning som reglerar när personnummer ska användas och inte användas. Det är inte alltid möjligt att identifiera personer med personnummer, om någon inte har något personnummer kan reservnummer användas. Reservnummer kan också användas om man av någon anledning inte vill ange patientens personnummer.

Informationssäkerhetsansvarig (B): Personnummer eller reservnummer kan användas för identifiering. Reservnummer används om personnummer inte finns t.ex. en utländsk person. Det finns egentligen bara ett tillfälle man kan vara anonym i vården och det är vid HIV test. Då får patienten ett löpnummer som de ska ange när de ska få resultatet. Visar det sig att de har HIV måste de identifieras.

Systemutvecklare (B): Personnumret används för identifiering. De använder inte pseudonymer.

6.2.3 Patienternas möjlighet att begränsa behandling av personuppgifterna i andra IT-system

IT-säkerhetsansvarig (A): Patientjournalsystemet har kopplingar till en mängd olika system där man tar med information på olika sätt. Respondenten säger att man enligt lag ska kunna

begränsa behandlingen av personuppgifter i andra IT-system, men respondenten vill påstå att patientjournalsystemet inte har det idag eftersom det är ett gammalt system.

Kravanalytiker (A): Kravanalytikern hänvisar till deras kunder hur patienterna har möjlighet att begränsa behandlingen av personuppgifter i andra IT-system, men säger att informationen till patienter är riktigt intressant om man ser till de tillsyner som gjorts av datainspektionen, där i princip alla granskade vårdgivare som använder sig av sammanhållen journal har bommat på den punkten. Det är för dålig information till patienterna.

Informationssäkerhetsansvarig (B): Patienten kan spärra sina uppgifter. Patienten kan inte motsätta sig att de behandlar uppgifterna, det är lagstiftat. Patienter kan inte gå till läkaren och sedan säga att vårdgivaren inte får skriva in besöket. Det står tydligt i lagen att de får behandla personuppgifter även om personen motsätter sig det. Det måste de göra för att kunna ge en god och säker vård. Det patienter kan göra är att spärra uppgifterna för någon som är utanför vårdenheten eller vårdgivaren. Patienter kan spärra att vara åtkomliga från en klinik. I äldre system funkar inte den funktionaliteten riktigt, så det är någon som landstingen jobbar på att förbättra.

IT-strateg (B): Respondenten svarade att patienter har rätt att spärra information.

6.3 Åtkomst i IT-system

I avsnittet presenteras resultatet från frågorna angående hur de säkerställer att IT-systemens användare har åtkomst till rätt information.

6.3.1 Begränsa användare åtkomst till fel information

IT-säkerhetsansvarig (A): I dagsläget har de olika klinikerna egna databaser. På exempelvis ett sjukhus finns det ca 24 olika databaser. Detta för att göra en segmentering och begränsa åtkomst. Allt detta arbetar de bort nu, tanken är att ha allt på ett och samma ställe och komma åt information till alla patienter centralt. Det som har gjort detta möjligt är patientdatalagen. Här skulle respondenten vilja påstå att man arbetar åt andra hållet, d.v.s. att mer patientdata blir tillgänglig.

Användaren har alltid tillgång till patientjournalerna. Respondenten har svårt att se hur de ska kunna styra när användaren ska arbeta eller inte arbeta med patientjournalerna. Respondenten tillägger att om en användare är på en annan arbetsplats är det inte säkert att den datorn har det nödvändiga programmet för att kunna nå patientjournalerna.

Kravanalytiker (A): Patientdatalagen förordar det aktiva valet som gör att användare får tillgång de behörigheter som verksamhetschefen bedömt att de borde ha. I patientjournalsystemet ges de möjlighet att selektera ut vilken information som ska kunna nås utan användaren gör ett ytterligare aktivt val när de öppnar journalen. Ett aktivt val är att öppna journalen och då får användaren tillgång till den informationen som finns sparad på vårdenheten. Det är det kunderna primärt bedömer att användaren behöver för att kunna utföra sitt arbete. Sen ger de möjlighet med stöd ifrån patientdatalagen att göra ett till aktivt val när användaren behöver mer information som ligger på andra ställen än där de jobbar. Det kan vara att användaren jobbar på medicin avdelning och användaren vill komma åt information på kirurgavdelningen. Då kan användaren göra ett ytterligare aktivt val för att få tillgång till den informationen. Ett aktivt val behövs för att få tillgång till mer information, användare får inte allt på en och samma gång. Det som anses som fel information här är fel

information vid fel tillfälle. Det vill säga att användaren ser mer än vad som behövs för att utföra arbetet. Detta gör att inte överflödig information visas. Utan användaren ser lite information först och behöver användaren mer får de välja det så de hamnar på rätt nivå.

Personuppgiftsombud (A): Det är en svår problematik att begränsa användare åtkomst till fel information. Åtkomst ska styras av behörigheter. De jobbar utefter tillgänglighet, spårbarhet, sekretess och riktighet inom informationssäkerhet. Anställd ska komma åt det som behövs för att utföra sitt arbete. Dessa behörigheter kontrolleras varje år vid medarbetarsamtal med cheferna. Där man checkar av vilka behörigheter de anställda har. De har kanske några som ska ta bort, eller några som ska läggas till. De ser hela tiden till att användaren har de behörigheter de behöver men inte fler.

Informationssäkerhetsansvarig (B): Det är en svår problematik att begränsa användare åtkomst till fel information för att man har en teknisk behörighet som gör att man kan komma åt mycket information. Det finns information som verkligen är inlåst, och det är exempelvis kvinnofridsenheten. Den är sekretessklassad inom landstinget så att bara kvinnofridsenheten kommer åt den. Sedan finns det även barnskyddsteam där det är känsligare.

Det finns en teknisk behörighet som gör att användare kommer åt mycket patientdata om patienterna och det beror på att man inte riktigt vet vilka uppgifter som behövs innan man ger patienten vård. Sedan har man olika urval i patientjournalsystemet. Olika vyer används för att inte komma åt patientuppgifter som inte behövs. Patientuppgifter görs tillgängliga stegvis. Användare får alltså inte allt framkastat framför sig. Utan att de måste göra aktiva val vad det är de ska ta del av. Exempelvis på första steget ser användaren sin enhets anteckningar, sedan kan användare se att patienten har uppgifter på ortopeden då kan de välja att öppna den vyn och läsa den informationen om användaren gör den bedömningen att den informationen har betydelse för vården av patienten. Men rent generellt har de ett problem i vården och det är att rent tekniskt begränsa behörigheten för att de inte riktigt vet vilka patienter som kommer in och när. Här finns en utmaning som de jobbar med. Användarna har alltid tillgång till patientjournalsystemet.

IT-strateg (B): Användaren har en användarroll och en behörighet. Utifrån behörighets matris har användaren tillgång till de delar av journalen som de behöver ifrån den enheten.

6.3.2 Begränsa systemadministratörer att läsa personuppgifter

IT-säkerhetsansvarig (A): Systemadministratörerna har full access till databaserna vilket gör att de kommer åt all information. Respondenten säger att kryptering är ett ord de inte känner till när det gäller patientjournalsystemet. De jobbar för att ta fram en krypterad lösning. Men respondenten vågar inte säga till vilken version, eller när i tiden.

Informationssäkerhetsansvarig (B): Databaserna är behörighetsstyrda på systemadministratör nivå. Enbart de som arbetar med databaserna kommer åt dem. Det kommer alltid att finnas ett antal systemadministratörer som kommer åt dessa. Detta kontrolleras dock genom loggar. Respondenten är osäker på om databaserna är krypterade. De litar på fysiska och administrativa skydd (att bara vissa administratörer har behörighet). Respondenten säger att det finns en fara med kryptering, dels är det nyckelhanteringen och dels är det väldigt stora datamängder, så det blir lätt ganska mycket belastning på systemen om man skulle kryptera lagringen.

IT-strateg (B): Respondenten svarade att det var fel person att fråga hur systemadministratörer begränsas att läsa personuppgifter.

6.4 Skydda uppgifterna

I avsnittet beskrivs hur uppgifterna skyddas ifrån obehöriga.

6.4.1 Autentisering

IT-säkerhetsansvarig (A): Användarnamn och lösenord används för autentisering i patientjournalsystemet. Det finns även andra system som är ihopkopplade med patientjournalsystemet. Det räcker då att vara inloggad i patientjournalsystemet för att komma åt information i de andra systemen.

Informationssäkerhetsansvarig (B): Användarnamn och lösenord används för autentisering i patientjournalsystemet. Respondenten säger att i dagsläget har de ingen stark autentisering till journalen. Den regel som finns är att om de för över känsliga uppgifter på ett öppet nät ska det krypteras. Respondenten hoppas att man ska få starkare autentisering inom något år eller två.

Systemutvecklare (B): Inloggningen är via Mina vårdkontakter där patienter loggar in med BankID.

6.4.2 Kryptering

IT-säkerhetsansvarig (A): Den enda nätverkskommunikationen som är krypterad är det trådlösa nätverket, mellan accesspunkten och klienterna.

Informationssäkerhetsansvarig (B): Ingen kryptering i nätverket men den diskussionen förs.

Systemutvecklare (B): Respondenten säger att all kommunikation med patientjournalsystemet på nätverket sker via certifikat så det är ingen öppen trafik på nätverket.

IT-strateg (B): Respondenten svarade att det var fel person att fråga angående kryptering.

Eftersom det inte fanns någon kryptering i databaser eller intern nätverkstrafik, är det inte några krypteringsnycklar som behöver hanteras. Nyckelhanteringen till applikationen för direktåtkomst på nätet är oklar.

6.4.3 Säkerhetsrutiner till IT-systemens användare

IT-säkerhetsansvarig (A): Användarna får utbildning inom säkerhet. Varje sjukhus eller förvaltning har eget ansvar för det, så det ser lite olika ut beroende på vilken förvalting det är, både IT-mässigt och informationsmässigt.

Personuppgiftsombud (A): De har en säkerhetspolicy i regionen. Eftersom det är regionen som skriver den, är det de som följer upp den. Respondenten påpekar att det finns regionalt reglemente, riktlinjer och anvisningar för informationssäkerhet som de följer. Respondenten säger att deras lokala rutiner följer dessa. De är ute och informerar och håller utbildningar och försöker följa upp så mycket de kan.

Informationssäkerhetsansvarig (B): Det finns en säkerhetspolicy. När personen anställs får de skriva på sekretessavtal som är en viktigt bit. Det finns utbildningar till patientjournalens användare om säkerhet. Både att folk kommer ut och utbildar men även att det finns

utbildningar på nätet. De tittar på hur många som har gått kurser. Diskussionen förs om att ha obligatoriska kurser, men det har de inte fått igenom.

IT-strateg (B): Säkerhetspolicy finns. Nyanställda får alltid utbildning och information om säkerhet. Utbildningar sker även fortlöpande. Respondenten säger att de har uppföljning i vissa moduler och tillägger att det sker beroende på om det är lättarbetat eller inte. Vidareutbildning finns, men de kontrollerar inte om användarna faktiskt kan systemet fullt ut. Det är supporten som tar det om det kommer upp frågor.

6.4.4 Loggning

IT-säkerhetsansvarig (A): Det respondenten känner till om vad som loggas är användaren, åtkomst till specifik patient, tid och datum. Möjligtvis att det de skriver i journalen loggas (men osäker). Respondenten skulle vilja säga att loggningssystemet är på en väldigt simpel nivå. De som kommer åt loggarna är systemadministratörer och utsedda personer ute i förvaltningarna. Respondenten känner inte till när säkerhetskopior av loggarna tas, eller när loggar raderas.

Personuppgiftsombud (A): Loggarna sparas i 10 år.

Informationssäkerhetsansvarig (B): I journalsystemen loggas användaren, patient, tidpunkt, vad de tagit del av m m. Loggarna är inte krypterade i dagsläget. Respondenten vet inte när loggarna säkerhetskopieras. Loggar måste sparas i 10 år.

IT-strateg (B): Respondenten vet inte hur loggarna är skyddade.

Systemutvecklare (B): De har gjort en integration mot ett system på landstinget som kallas för X som i sin tur går via patientjournalsystemets loggar. Där loggas vem som öppnat vilka journaler. Användaren kan se vilken vårdpersonal som läst deras journaler. De gör själva inga lagringar i deras applikation utan de läser enbart från loggningen som finns i X.

6.4.5 Förvaring av backuper

IT-säkerhetsansvarig (A): De har en väldigt stor backuplösning som är centraliserad och det finns redundans på backuperna på flera olika ställen. Det är osäkert på om de är lagrade på band fortfarande men backuperna är inlåsta i skåp.

Informationssäkerhetsansvarig (B): Respondenten vet inte hur backuper förvaras.

IT-strateg (B): Respondenten är osäker på hur backuper lagras.

6.4.6 Avveckling av lagringsmedia

IT-säkerhetsansvarig (A): När de stora mängderna lagringsmedia i exempelvis Network Attached Storage (NAS) ska avvecklas, har de avtal med ett stort företag som också levererar de vanliga datorerna. De har även interna rutiner hur dumpster diving ska undvikas, och hur lagringsmedia ska förstöras. De har även egna system för att slå sönder den elektroniska informationen

Informationssäkerhetsansvarig (B): Lagringsmedia destrueras antingen av dem själva, eller av den firma som de har avtal med för destruktion. De lämnar inte vidare eller säljer inte vidare något.

6.4.7 Beredskapsplan för oförutsedda händelser

IT-säkerhetsansvarig (A): Beredskapsplanen för oförutsedda händelser skulle respondenten vilja dela upp det i två olika delar när det gäller patientjournalsystemet; det som finns på datorer och det som finns på servrar. Det som är intressant är det som finns på servrar. Respondenten säger att det finns olika typer av kontinuitetsplaner och rutiner om hur man ska gå tillväga om någon oförutsedd händelse sker. Det finns inte exakt redovisat hur man ska återställa specifika händelser, det beror mycket på olika faktorer. Respondenten hävdar att man har erfarenhet av alla händelser (se bilaga A) och har kunnat hantera detta.

Informationssäkerhetsansvarig (B): De har en incidenthanteringsplan för oförutsedda händelser. De systemansvariga har rutiner för hur de ska återställa data när det händer något. Sen har de inte gjort någon större skillnad om det är brand eller datavirus. Det hanteras med incidenthanteringen.

6.4.8 Intrångsdetektering och otillåten åtkomst

IT-säkerhetsansvarig (A): Det finns en stor förbättringspotential i kontroller av intrångsdetektering och otillåten åtkomst. Givetvis upptäcker de en del. De som har tillgång till loggarna gör stickprovskontroller för att kontrollera att användarna som är inne i systemen har varit inne på rätt sätt. Respondenten tror dessa stickprovskontroller behöver förbättras.

Informationssäkerhetsansvarig (B): De har slumpmässiga logguppföljningar för att kontrollera otillåten åtkomst. Landstinget har ca 100st per år centralt där de tar ut vad användarna tagit del av. Dessa går de sedan igenom med chefen.

Sen finns det tillfällen när verksamheten själv gör kontroller. Exempelvis när de fått in en person med högt nyhetsvärde. Mordet på Anna Lindh är ett sådant exempel. Verksamhetschefen gör då själv logguppföljning. Samma kontroller görs om det finns en hotbild mot patienter. Det är ca 150 patienter som kollar sin logg varje dag via nätet. I övrigt är det gatewayen som hanterar intrångsdetektering om någon försöker ta sig in på det sättet. Respondenten tror inte att sådana försök är vanliga dock.

6.5 Låt IT-systemen styra användaren rätt

Resultat om utformning av IT-system för att styra användaren i rätt riktning.

6.5.1 Borttagning av onödig data

IT-säkerhetsansvarig (A): I patientjournalsystemen får man inte lov att ta bort någon information om man inte fått beslut från Socialstyrelsen att göra det. Så fort en anteckning gjorts är det en journalanteckning. Då får inte, kan inte, ska inte, anteckningar kunna tas bort. Det händer någon gång då och då att anteckningar behöver tas bort, och det är en ganska krånglig procedur där de egentligen måste ta in leverantören av systemen, för att gå in på något sätt och ta bort anteckningen.

Informationssäkerhetsansvarig (B): De får enbart ta bort uppgifter om Socialstyrelsen beslutat det. Det finns rutiner hur det ska göras. De ska egentligen ta bort data i alla backuper då också, men det tror inte respondenten är genomförbart idag, det är ett litet problem.

6.5.2 Utformning av användargränssnitt

IT-säkerhetsansvarig (A): Användargränssnittet är inte utformat så det begränsar inmatning av sådant som inte får skrivas in. Tyvärr bygger idag väldigt många av de anteckningar som görs på fritextfält.

Kravanalytiker (A): Patientjournalsystemet har begränsningar i inmatningen av vissa datatyper i vissa fält men det är snarare ur ett informationsstrukturellt syfte, snarare än integritetssyfte. Det de enkelt kan göra idag är exempelvis att förbjuda bokstäver i ett fält där det ska vara personnummer.

Men den egentliga integritetskänsliga informationen i journalen, som man kanske av spärrskäl vill ha i vissa poster och inte i andra, kommer oftast i text vilket gör det svårt att begränsa. För det man skulle vilja begränsa är exempelvis att läkemedelsinformation om patienter skrivs in i en post eller anteckningstyp som klassas som läkemedelsinformation. För när man sedan ska registrera spärren, kan man välja om detta ska följa med eller inte. Så hade de velat göra men de har funnit det ganska svårt.

Informationssäkerhetsansvarig (B): Vissa diagnoser kan bara sättas på kvinnor och några bara på män, då är det inmatningsbegränsningar. Men nu fick de en kvinna som gjort om sig till man och fick manligt personnummer. Då blev det problem för då kan de inte vårda personen då han blev gravid. Det är lite svårt. I fritextfälten har de inga begränsningar. Men där det går, försöker de ha inmatningsbegränsningar.

6.5.3 Insamling av samtycke

Personuppgiftsombud (A): Insamling av samtycke är något som kommer tillsammans med sammanhållen journalföring. Regionen har gått ut med information till verksamheter. Informationsblad m m kan hämtas/beställas på nätet. Affischer finns framtagna. Information och rutiner finns på regionens hemsida.

Kravanalytiker (A): Det finns ingen spärr i patientjournalsystemet som förhindrar att data skrivs in om samtycke inte erhållits. Behovet av en ruta som kan bockas i när samtycke samlats in, har inte kommunicerats av deras kunder och de har inte heller sett något behov av att införa det.

Informationssäkerhetsansvarig (B): Samtycke samlas in i samband med möten med patienten.

IT-strateg (B): Samtycke samlas in vid möten och remiss.

6.5.4 Information till patienter hur uppgifter kommer behandlas

Personuppgiftsombud (A): Patienten får information om hur uppgifterna kommer behandlas muntligt, ibland skriftligt och ibland via uppsatta affischer i t ex väntrum. Vid forskning gäller nästan alltid skriftlig information plus samtycke.

Kravanalytiker (A): Det finns inte någon ruta som kan bockas i som säger att vårdgivaren har informerat patienten angående hur uppgifter kommer behandlas. Kravanalytiker säger dock att det inte vore en dum ide att införa.

Informationssäkerhetsansvarig (B): Patienten får information hur om uppgifterna kommer behandlas vid möten, via anslag i väntrum och kallelser.

IT-strateg (B): Patienten får information hur om uppgifterna kommer behandlas; muntligt, även på internet, väntrum osv.

6.5.5 Anonymisering till forskning, rapporter och statistik

IT-säkerhetsansvarig (A): Respondenten tror att det handlar ganska mycket om manuellt arbete, om utdrag ur patientjournalsystemet behövs till exempelvis forskning eller statistik.

Kravanalytiker (A): De har inte särskilt bra stöd för elektronisk utlämning idag. De landsting som exempelvis lämnar ut information till forskare, skriver ut på papper och anonymiserar helt manuellt vad respondenten hört. Där finns inget bra stöd idag eftersom det inte har varit prioriterat från deras kunder, men nu har det ändrats. De håller på att arbetar fram en riktig funktion för elektronisk utlämning där anonymisering uppkommit som ett behov i kravdiskussionerna.

Personuppgiftsombud (A): För att få begära ut data till forskningsprojekt måste man först få ett godkännande. Det går för det mesta via etikprövningsnämnden där man samlat in samtycke ifrån patienten eftersom det finns informationsskyldighet. För att anonymisera patienten används kodnycklar. Patienten har en kod som ersätter namn och personnummer. Nyckeln sparas separat och är inlåst.

Informationssäkerhetsansvarig (B): Utlämning av patientdata är möjligt efter det att patienten gett sitt samtycke till studien. Forskare får först ansöka till etikprövningsnämnden för att få godkänt till sin studie. Sedan beror det på vad de behöver, men det går att få ut anonymiserade rapporter. De har en utdataenhet som tar ut statistik och utdrag. De kan anonymisera men det sker inte automatiskt i systemet.

IT-strateg (B): De har en roll i journalsystemet som heter Monitorerare som anonymiserar data.

6.6 Transparens

Avsnittet beskriver hur och till vilken grad patienter har insyn i patientjournalsystemen.

IT-säkerhetsansvarig (A): För att se vad som finns sparat om patienter får de begära ut det via pappersvägen. Respondenten har väldigt svårt att se att de skulle ta fram en lösning som ger medborgare direktåtkomst till registrerad information för existerande patientjournalsystem. Respondenten känner inte till att det finns för det patientjournalsystemet någon annanstans. Respondenten tror att om man ska ha en sådan lösning behöver man ha ett helt annat system. Respondenten tror inte det är aktuellt att bygga något på existerade patientjournalsystem.

Kravanalytiker (A): Transparens är i första hand en fråga till landstinget. Respondenten tar upp applikationen som Landsting B använder. Att det är en relevant fråga till landstingen med särskild tanke på att många som är inne i det projektet nu. I de landsting man faktiskt har börjat med detta, har det blivit ett drag med anmälningar till myndigheter.

På frågan om företaget utvecklar något liknande internetjournal, säger respondenten att de tittar på möjligheter att ansluta sig till applikationen Landsting B använder. Där är de ganska styrda av de regler som finns kring det systemet. De utvecklar inget eget.

Informationssäkerhetsansvarig (B): Transparens har de via applikationen, men det är egentligen inte hela journalen. I dagsläget är exempelvis inte psykiatrijournalen med. Det är en del som de lämnar ut via applikationen. Sen kan patienten begära att få ett registerutdrag via pappersvägen. Patienten kan se vem som tagit del av deras journal, men inte vem som skrivit in det via applikationen. Det kan de dock om de begär ut den via pappersvägen. De håller på att föra samman logginformation med nationell patientöversikt, så patienter kan delvis se vilka andra organisationer som tagit del av informationen.

IT-strateg (B): Patienter kan läsa sin journal men det är inte alla journaler. Det är filtrerat beroende på ett regelverk, så vissa enheter är bortfiltrerade, exempelvis psykiatrin. Patienter kan läsa diagnoser, läkemedel, remisser, remissvar, labbsvar, patientdata (namn, adress, mail, anhöriga). Patienter kan se vem som skrivit in anteckningen, datum, namn på personen och vilken roll (läkare, sekreterare). Den är dock mer begränsad än de stora loggar där man exempelvis kan se hur länge personer har vart inne på en sida. Patienter kommer i framtiden kunna se om det finns spärrar i journalen.

Systemutvecklare (B): När patienter loggar in på nätet används deras för- och efternamn för att presentera patienten. Via applikationen får patienten tillgång till journalanteckningar, diagnoser, provsvar, remisser, kontakter med vården, läkemedel och kan läsa loggrapporter för att se vem som öppnat deras journaler.

Personnumret måste lagras för det används för några integrationer som de har bland annat mot ett personregister där de plockar ut länstillhörighet.

6.7 Kända brister

Respondenterna blev tillfrågade om problem ur integritetssynpunkt med IT-systemen.

IT-säkerhetsansvarig (A): Patientjournalsystemet är lappat, lagat och ändrat och respondenten tror inte det är någon idé att fortsätta med det. Vad man egentligen borde göra är att byta ut patientjournalsystemet till något nyare system som har stöd för fler funktioner, exempelvis transparens där patienten kan nå sin journal via nätet.

Kravanalytiker (A): Det största integritetsproblemet egentligen som systemet bidrar till, är att den gällande lagstiftningen utgår från ett organisatoriskt perspektiv som tar mer hänsyn till var information finns, än i vilket sammanhang den behövs. Säg att en användare jobbar på medicin och behöver information på kirurgen, då bryter användaren den inre sekretessen för det har användaren rätt till, men användaren får se allt som finns på kirurgen och inte bara det som ingår i den process som ska behandlas. Detta är ett jätte integritetsproblem, och systemen är uppbyggda på det sättet. Det vill säga att information binds till den vårdenhet där den hör hemma. Ska man tillgodogöra sig mer information som man har rätt till, i 9 av 10 fall tillgodoser man sig för mycket information. Skulle respondenten vilja ändra något med journalsystemet, skulle respondenten lägga ett större fokus på vårdprocess. När man gör ett aktivt val att tillgodose sig mer information någonstans, vill man ha den information som matcher den process som man själv är inblandad i. Man kanske bara vill ha information som har att göra med armen men på kirurgen fanns det även information om benet, huvud och blindtarmen. Det är det största integritetsproblemen de har idag.

Personuppgiftsombud (A): Det finns alltid förbättringsmöjligheter. Detta är en fråga som är under arbete hela tiden för att förbättra systemet. En synpunkt som kom in nyss från läkare,

var att de ska vara enklare att kunna avidentifiera. Patientjournalsystem A är väldigt mycket under utveckling nu för att möta upp de lagar som finns mer och mer.

Informationssäkerhetsansvarig (B): Det borde vara enklare att bara ta del av just det man behöver, att minska mängden överskottsinformation. Man ska på ett enkelt sätt kunna välja vad man har behov av. Nackdelen nu är att det blir väldigt många klick på många olika ställen. Det är ett problem som de jobbar med.

IT-strateg (B): När man har samlad patientjournal och många vårdgivare är det många som kan ta del av journalen, men det finns säkerhetsaspekter. Det blir ur patientsynpunkt säkrare eftersom information finns tillgänglig vid rätt tillfälle, men risken ökar att de kan ta del av för mycket information. Men lagen säger ändå vad man får göra och inte göra.

Systemutvecklare (B): De lagrar enbart tre personuppgifter i deras databas: personnummer, för- och efternamn. Det är personnumret som är kopplat till användaren. De enda som kan komma åt dessa personuppgifter är administratörer på databasen. Patientdata läser de från patientjournalsystemet så de lagrar inga journaldata själva.

7 Analys

I detta avsnitt har resultatet analyserats ifrån den informationen som kommit fram via telefonintervjuerna med de sex respondenterna. Avsnittsindelningen är samma som i resultatavsnittet. Tabell 1 ger en överblick på hur de båda landstingen uppfyller de fem områdena inom PbD som studien har analyserat. En mer utvecklad text följer efter tabellen.

Tabell 1 Kort sammanfattning av analysen.

	Landsting A	**Landsting B**
Minimera mängden personuppgifter.	Patientjournalsystemet följer delvis PbD. Vid utveckling av nya funktioner selekterar kravanalytiker efter behovet ut vilka uppgifter som ska kunna sparas i patientjournalsystemet. Patienter kan identifieras med pseudonymer. Inga funktioner för att spärra personuppgifter i andra IT-system.	Patientjournalsystemet följer delvis PbD. Patienter kan identifieras med pseudonymer. Inga funktioner för att spärra personuppgifter i andra IT-system.
Begränsa åtkomsten till uppgifterna.	Patientjournalsystemet följer inte PbD. Användarna kan tillgodose sig mer information än de behöver. Finns dock begränsningar som gör att användarna måste göra aktiva val för att ta del av mer information.	Patientjournalsystemet följer inte PbD. Användarna kan tillgodose sig mer information än de behöver. Finns dock begränsningar som gör att användarna måste göra aktiva val för att ta del av mer information.
Skydda uppgifterna.	Patientjournalsystemet följer inte PbD. Ingen kryptering i varken databaser eller intern nätverkstrafik. Stickprovskontroller för att kontrollera åtkomst till patientjournalerna. Finns rutiner för att destruera lagringsmedia.	Patientjournalsystemet följer inte PbD. Ingen kryptering i varken databaser eller intern nätverkstrafik. Stickprovskontroller för att kontrollera åtkomst till patientjournalerna. Finns rutiner för att destruera lagringsmedia.
Låt systemen styra användaren rätt.	Patientjournalsystemet följer inte PbD. Enbart begränsningar för datatyper i vissa fält. Inga begränsningar i fritextfältet där det mesta av journalföringen görs.	Patientjournalsystemet följer inte PbD. Enbart begränsningar för datatyper i vissa fält. Inga begränsningar i fritextfältet där det mesta av journalföringen görs.

Transparens.	Patientjournalsystemet följer inte PbD. Inget stöd för direktåtkomst till patientjournaler.	Patientjournalsystemet följer PbD filosofin. Patienter har direktåtkomst till sin journal på nätet.

7.1 Presentation av respondenter

Alla sex av de intervjuade respondenterna har eftergymnasial utbildning. Fyra av respondenterna har olika administrativa och tekniska utbildningar på högskolor och universitet. En är utbildad systemvetare, de andra tre har läst kurser och utbildningar inom data, matte, vårdmanagement, IT-projektledning, hälso- och sjukvårdsadministration, hälso- och sjukvårdsjuridik och verksamhetsuppföljning. En av respondenterna är utbildad inom vården.

Respondenterna har jobbat med sin roll mellan sex och ett år. En av respondenterna har haft en liknande roll på ett konkurrerande företag.

7.2 Minimering av personuppgifter som samlas in i IT-system

Avsnittet presenterar resultatet från hur landstingen och patientjournalföretagen gör för att minska antalet personuppgifter i IT-systemen.

7.2.1 Minimera uppgifter som samlas in

PbD syftar på att IT-systemen ska vara utformade i förväg för att så få personuppgifter som möjligt hanteras, och fastställa att enbart de personuppgifter som krävs till ändamålet samlas in. På dessa punkter följer patientjournalsystemet (A) PbD. Personuppgifter som samlas in tillgodoser ändamålet och inget mer. Det framgår dock inte hur omfattande de efterföljande kontrollerna av patientjournalsystemen är.

Tyvärr lyckades enbart kravställare/kravanalytiker till patientjournalutvecklare på Landsting A intervjuas. Kravanalytikern berättar att de redan under utvecklingen av nya funktioner arbetar för att selektera ut så att uppgifterna enbart innefattar behovet. De agerar ”grindvakter” för vad som ska lagras eller inte lagras. Respondenten påpekar även att mer och mer resurser läggs för att rätta till saker i produkterna.

Två respondenter på landstingen säger att lagstiftningen styr vilka uppgifter som får samlas in i patientjournalsystemen och det är upp till användaren att följa detta. Verksamhetscheferna gör kvalitetssäkringar på datainsamlingen för att säkerställa att den är lämplig.

Minimeringen av personuppgifter som samlas in i Landsting A sker genom återkommande revisioner. Personuppgifter ska inte sparas längre än vad som är nödvändigt. De följer regionens dokumenthanteringsplan.

Applikationen för direktåtkomst till patientjournalen lagrar enbart för- och efternamn som används för att presentera användaren när de loggar in på sin journal. Personnumret används för att koppla användaren i patientjournalsystemet. Detta är uppgifterna de lagrar, alla patientdata läser de enbart ifrån patientjournalsystemen.

7.2.2 Uppgifter för identifiering

För att minska integritetsriskerna kan pseudonymer användas vilket görs i båda patientjournalsystemen. Patientjournalsystemen använder sig av reservnummer för identifiering. Reservnummer fungerar som en pseudonym och ersätter personnumret.

Applikationen för direktåtkomst till patientjournaler använder dock inga pseudonymer utan där används personnumret för identifiering.

7.2.3 Patienternas möjlighet att begränsa behandling av personuppgifter i andra IT-system

I Landsting A är det inte möjligt att begränsa behandlingen av personuppgifter i andra IT-system eftersom det är ett gammalt patientjournalsystem. IT-säkerhetsansvarig är medveten om att man enligt lag ska kunna göra sådana begränsningar.

Även i Landsting B funkar inte den funktionaliteten riktigt eftersom det är ett äldre system. Det patienterna kan göra är att spärra information.

7.3 Åtkomst till IT-systemen

IT-systemen ska vara utformade på ett sådant sätt så att enbart användare som arbetar med informationen ska ha åtkomst till den.

7.3.1 Begränsa användarnas åtkomst till fel information

Behörigheten ska vara anpassad så att användare enbart kommer åt de uppgifter de behöver för att kunna utföra sina arbetsuppgifter.

Användarna kan tillgodogöra sig mycket mer information än de behöver genom att göra aktiva val, vilket betyder att patientjournalsystemet inte följer PbD för att skydda patienternas integritet. Dock har begränsningar gjorts för att användarna inte ska få all information ”kastad framför sig”.

Användarna i patientjournalsystemen har en teknisk behörighet som gör att de kan komma åt mycket information. Användarna har från början behörighet inom sin enhet, eller den behörighet som användarna bedömt tillsammans med verksamhetschefen att de behöver för att utföra sina arbetsuppgifter. Sedan kan de göra ett aktivt val om de bedömer att de behöver mer information. Flera av respondenterna har svarat att det är ganska krångligt med behörighetsstyrning i patientjournalsystemen, eftersom de aldrig kan veta vilken information som behövs. Användarna har möjlighet att tillgodose sig med mer information, men det kräver dock att de gör ett aktivt val för att öppna fler vyer i patientjournalsystemet så de får inte allt framkastat framför sig.

7.3.2 Begränsa systemadministratörer att läsa personuppgifter

Kryptering kan användas som komplement till behörighetsstyrning. Kryptering kan hindra exempelvis systemadministratörer från att se personuppgifter under tiden de arbetar med IT-systemen. Kryptering används inte i något av patientjournalsystemen. Åtkomsten till informationen begränsas inte för systemadministrativ personal. På den punkten följer inte något av patientjournalsystemen PbD.

Systemadministratörerna har full access till databaserna. IT-säkerhetsansvarig säger att kryptering är ett ord man inte känner till när det gäller patientjournalsystemet i Landsting A. I patientjournalsystem (B) är respondenten osäker om databaserna är krypterade och någon

person som kan svara på frågan har inte gått att nå. I ett av patientjournalsystemet kontrolleras access till databasen via loggar, och man litar på fysiska och administrativa skydd.

7.4 Skydda uppgifterna

Personuppgifterna ska ifrån början vara skyddade med hjälp av säkerhetsfunktioner som autentisering, kryptering och fysisk säkerhet.

7.4.1 Autentisering

Ska systemen följa PbD är minimikravet att lösenord och tillhörande rutiner används.

Båda patientjournalsystemen använder sig av användarnamn och lösenord för att autentisera användarna. Det vill säga att vårdpersonalen behöver användarnamn och lösenord för att få tillgång till patientjournalerna.

När medborgare ska använda applikationen för direktåtkomst till patientjournaler är inloggningen via ”Mina vårdkontakter” där de loggar in med BankID.

7.4.2 Kryptering

Kryptering kan användas på flera ställen som databaser och i nätverket för att skydda uppgifterna. Här finns det stora brister vilket gör att trafik kan avlyssnas och data kan läsas vid stöld av hårddiskar. Principerna i PbD används inte alls på punkten för att skydda patientens integritet.

På punkten att begränsa systemadministratörer att läsa personuppgifter, svarade en av respondenterna att det inte var kryptering i databaserna, och i det andra patientjournalsystemet var det osäkert.

På Landsting A uppger respondenten att ingen nätverkskommunikation förutom det trådlösa nätverket är krypterat. På Landsting B är ingen intern nätverkskommunikation krypterad men diskussionen förs.

Eftersom det inte fanns någon kryptering i databaser eller intern nätverkstrafik är det inte heller några krypteringsnycklar som behöver hanteras.

Vid kommunikation mellan applikationen för direktåtkomst på nätet och patientjournalsystemet används certifikat. Nyckelhanteringen för applikationen är oklar.

7.4.3 Säkerhetsrutiner till IT-systemens användare

Det ska finnas rutiner och information till IT-systemens användare om säkerhet för att skydda patientens integritet. Punkten är svår att analysera eftersom det fungerar olika på förvaltningarna. Ett framtida arbete skulle kunna vara att kontrollera detta på olika förvaltningar.

Personuppgiftsombud i Landsting A säger att det finns regionalt reglemente, riktlinjer och anvisningar för informationssäkerhet som de följer. Deras lokala rutiner följer dessa. De är ute och informerar och håller utbildningar och försöker följa upp så mycket de kan.

Rutinerna och informationen ser lite olika ut beroende på vilken förvaltning det är. Det finns säkerhetspolicys och användarna får alltid utbildning och information vid nyanställning men

även efteråt. På landsting B har diskussioner förts om obligatoriska utbildningar men det har inte gått igenom än.

7.4.4 Loggning

Genom att kontrollera loggar kan felaktig åtkomst till personuppgifter av användarna upptäckas. Loggarna är en fristående del, och kan även de vara en säkerhetsrisk. Det är därför viktigt att även de skyddas. Loggarna kan användas för att spåra vilka användare som varit inne i loggarna. Dock är inte loggarna krypterade vilket utgör en integritetsrisk i sig eftersom även de innehåller information.

I journalsystemen loggas användare, patient, tidpunkt, vad de tagit del av, vem som skrivit in vad (osäkert i ett av systemen). Respondenten i Landsting A säger att loggsystemet är på en väldigt simpel nivå. Loggarna sparas i 10 år.

7.4.5 Förvaring av backuper

Backuper innehåller mycket information och bör vara skyddade både genom kryptering och fysisk säkerhet. Ingen av respondenterna har kunnat svara på om de är krypterade men backuperna är inlåsta på något sätt.

7.4.6 Avveckling av lagringsmedia

Destruering av lagringsmedia kan förhindra att data läcker ut på grund av att någon obehörig får tillgång till lagringsmedian när de inte längre används. Båda landstingen har kontroll på hanteringen av lagringsmedian när den avvecklas vilket förhindrar att data läcker ut.

I båda landstingen finns rutiner för hur lagringsmedia ska förstöras när den inte används längre och båda landstingen har även avtal med det företag som de köpt utrustning ifrån där de kan få hjälp att ta hand om utrustningen.

7.4.7 Beredskapsplan för oförutsedda händelser

Hårddiskar och annan lagringsmedia kan gå sönder när som helst. Förvaltningar kan även drabbas av bränder, översvämningar, virus eller andra hot som gör att data går förlorad. Beredskapsplanerna har inte analyserats i detalj men planer för återställning av data finns i båda landstingen.

Båda landstingen har rutiner och incidenthanteringsplan hur man ska återställa data när lagringsmedia går sönder. På Landsting A att de historiskt sett haft alla incidenter (se bilaga A) och lyckats hantera dessa.

7.4.8 Intrångsdetektering och otillåten åtkomst

Att obehöriga inte får tillgång till data bör alltid kontrolleras under tiden som IT-systemen är aktiva. Kontroller görs men de är väldigt små och bristfälliga.

IT-säkerhetsansvarig på Landsting A säger att här finns en ganska stor förbättringspotential. Det görs stickprovskontroller för att se att användarna har varit inne på rätt sätt i patientjournalsystemen.

Även på Landsting B görs slumpmässiga logguppföljningar. Det rör sig om ca 100 st per år inom landstinget. Eftersom patienterna i landstinget har direktåtkomst till sin journal via nätet, kan de även se visningar på journalen själva. Detta görs dagligen av ca 150 personer. I övrigt är det gatewayen som hanterar intrångsdetektering om någon försöker ta sig in på det sättet. Respondenten tror dock inte att sådana försök är vanliga.

7.5 Låt IT-systemen styra användaren rätt

För att integritetssäkra IT-system är det viktigt att de är användarvänliga och styr användaren i rätt riktning.

7.5.1 Borttagning av onödig data

När data inte längre behövs ska verksamheterna ta bort datan. Funktioner för att radera uppgifter automatisk underlättar. Borttagning av data är en krånglig procedur eftersom leverantören måste kallas in. Det kan leda till att uppgifter inte raderas alls.

Respondenterna i de båda landstingen svarar med att man inte lov att ta bort någon information i patientjournalsystemen om det inte är så att man fått beslut ifrån Socialstyrelsen att göra det. Så fort en anteckning gjorts är det en journalanteckning. Då får inte, kan inte, ska inte, anteckningar kunna tas bort det. Det händer någon gång då och då att anteckningar behöver tas bort, och det är en ganska krånglig procedur där man egentligen måste ta in leverantören av systemen för att gå in på något sätt och ta bort anteckningen.

På Landsting B ska de egentligen ta bort data i alla backuper då också, men en respondent tror inte det är genomförbart idag. Anses vara ett litet problem.

7.5.2 Utformning av användargränssnitt

Användargränssnittet ska vara utformat så det inte går att mata in sådant som inte får skrivas in. Anteckningarna görs via fritextfält där det inte finns några begränsningar.

Det som finns är att vissa datatyper inte går att skriva in i vissa fält. Mycket av inmatningen om patienter kommer ofta i fritextfält vilket gör det svårt att begränsa vad som skrivs.

7.5.3 Insamling av samtycke

För att registrera information måste samtycke samlas in ifrån patienterna. Patientjournalsystemet (A) har ingen funktion för att förhindra att information skrivs in innan de erhållit samtycke. Till patientjournalsystemet (B) har inte något svar kommit.

Insamling sker vid möte med patienten och remisser.

7.5.4 Information till patient hur uppgifter kommer behandlas

Patienterna ska ha tydlig information som beskriver hur det som samlas in kommer att behandlas. De har informationsplikt p.g.a. personuppgiftslagen. Patientjournalsystemet (A) har ingen funktion för att kontrollera om patienten verkligen fått information om behandlingen om information. Till patientjournalsystemet (B) har inte något svar kommit.

Information sker framförallt i mötet med patienten. Det finns även affischer i väntrum, information på internet, och i kallelser.

7.5.5 Anonymisering till forskning, rapporter och statistik

När utdrag görs ur patientjournalsystemen ska informationen kunna anonymiseras. Data kan anonymiseras, men det görs helt manuellt så det finns inget stöd i patientjournalsystemen.

Landsting A håller på att jobbar med stöd för elektronisk utlämning.

7.6 Transparens

Transparens syftar på att ge registrerade insyn i IT-systemen. Patienterna ska kunna se vad som finns lagrat om dem i patientjournalsystemen. Funktionen finns enbart i Landsting B.

I Landsting A kan patienterna enbart begära ut sin journal via pappersvägen. På frågan om företaget utvecklar någon liknande internetjournal till kravanalytiker svarar respondenten att de tittar på möjligheter till anslutning till applikationen som Landsting B använder. Där är de ganska styrda av de regler som finns kring systemet, och utvecklar inget eget.

I Landsting B kan patienterna nå sin journal direkt via internet. Via applikationen får patienten tillgång till journalanteckningar, diagnoser, provsvar, remisser, kontakter med vården, läkemedel och kan läsa loggrapporter för att se vem som öppnat deras journaler. De kan dock inte se vem som skrivit in vad, utan måste då begära ut journalen via pappersvägen. Via applikationen kan de inte nå alla journalanteckningar. Det är filtrerat beroende på ett regelverk så vissa enheter är bortfiltrerade, exempelvis psykiatrin.

7.7 Kända brister

Alla respondenterna blev till sist tillfrågade om det finns några problem ur integritetssynpunkt med deras IT system som de tycker behöver åtgärdas.

IT-säkerhetsansvarig på Landsting A säger att patientjournalsystemet är lappat, lagat och ändrat och respondenten tror inte det är någon idé att fortsätta med det. Vad man egentligen borde göra är att byta ut patientjournalsystemet till något nyare system som har stöd för fler funktioner, exempelvis transparens där patienten kan nå sin journal via nätet.

Tre av respondenterna är inne på spåret att det är för lätt att ta del av för mycket information. PbD syftar på att det ska begränsas så det enbart omfattar ändamålet. Kravanalytiker i Landsting A säger att när man gör ett aktivt val att tillgodose sig mer information, vill man ha den information som matcher den process som man själv är inblandad i. Man kanske bara vill ha information som har att göra med armen, men på kirurgen fanns det även information om benet, huvud och blindtarmen. Det är det största integritetsproblemen de har idag.

Personuppgiftsombud i Landsting A säger att en synpunkt som kom in nyss ifrån läkare, var att de ska vara enklare att kunna avidentifiera. Patientjournalsystem A är väldigt mycket under utveckling nu för att möta upp de lagar som finns mer och mer.

Systemutvecklare i Landsting B nämnde inga brister.

8 Slutsats

Målet med studien var att besvara följande fråga:

”På vilket sätt används principerna och ramverket PbD i patientjournalsystem för att skydda patientens integritet?”

Slutsatsen diskuteras närmare i nästa avsnitt.

8.1 Diskussion

Enligt informationen som framkommit via intervjuerna med personer på landstingen, och personer på företagen som utvecklar patientjournalsystemen, används principerna och ramverket PbD på en del punkter i patientjournalsystemen, men det är även många punkter där de är långt ifrån PbD filosofin.

Minimering av personuppgifter som samlas in i IT-system följer PbD på flera punkter eftersom när funktioner utvecklas, selekteras enbart nödvändiga personuppgifter ut. Detta gör att insamlingen av uppgifter som inte behövs undviks. Båda patientjournalsystemen har även stöd för att använda pseudonymer. Dock finns ingen funktion för patienten att begränsa användningen av personuppgifter i andra IT-system för patienten.

Användarna kan tillgodose sig mycket mer information än de behöver genom att göra aktiva val, vilket betyder att patientjournalsystemet inte följer PbD för att skydda patienternas integritet. Dock har begränsningar gjorts så användarna inte får all information ”kastad framför sig”. Begränsningar är problematiska eftersom det är svårt att veta när information behövs. Respondenterna är medvetna om problemet. Givetvis skulle de kunna begränsa åtkomsten mer, men det betyder att vården blir lidande istället för integriteten, eftersom vårdgivarna inte får tillgång till lika mycket information om patienten vilket kan behövas till vården. Det är något som de inte vet hur det kan lösas på ett bra sätt. Frågan är om det ens är möjligt att följa PbD fullt ut på punkten.

När det gäller skydda uppgifterna har det framkommit flera brister då de intervjuade svarat att varken databaserna med patientdata, eller den interna nätverkstrafiken är krypterad, vilket är oroväckande. Inte heller kontrollen av otillåten åtkomst är bra då det enbart görs stickprovskontroller. Däremot är avveckling av lagringsmedia bra med avseende på skydd av uppgifter, då de har avtal med företag, och själva har verktyg för att destruera lagringsmedia.

Punkterna under rubriken ”Låt IT-systemet styra användaren rätt” följde inte PbD. Det finns få begränsningar för vad som kan matas in då det mesta är fritextfält. Det som begränsas är att hindra olika datatyper ifrån att skrivas in i vissa fält. Borttagning av data är krångligt eftersom de då måste ta in leverantören av patientjournalsystemet. Det finns inget som spärrar inmatning (A) av data tills samtycke samlats in. Samma sak gäller kontrollen om patienten tagit del av information om hur uppgifterna kommer behandlas. Det finns inte någon spärr där som blockerar att data skrivs in. Det finns inte heller något stöd för att anonymisera uppgifter till rapporter och forskning utan det måste göras manuellt.

Transparensen är det enda som skiljer sig mycket åt mellan de båda landstingen. Patienterna i Landsting A kan enbart begära ut journalerna via pappersvägen. I Landsting B har

medborgarna direkt åtkomst till sin journal via internet där de har tillgång till en del information som exempelvis vem som tagit del av deras journal.

Tre av respondenterna tar upp att det är för lätt att ta del av för mycket uppgifter när det tillfrågas om brister i patientjournalsystemen, PbD syftar på att det ska begränsas så det enbart omfattar ändamålet. Det tyder på en medvetenhet om bristerna.

8.1.1 Reflektion av egna arbetet

Intervjufrågorna mailades till respondenterna innan intervjutillfället. Detta för att respondenterna skulle veta vad för typ av frågar som skulle ställas, om det var sådana frågor som de kunde svara på. Detta gjordes också för att de kunde vara förberedda på vad de skulle svara på frågorna. Flera av respondenterna gjorde innan intervjun anteckningar för vad de skulle svara på frågorna. En återkoppling gjordes genom att skriva en sammanfattning där svaren tolkades och mailades tillbaka till respondenterna.

Det som har varit positivt med att använda intervju som metod är att flera av respondenterna har öppnat upp sig och förklarat detaljerat hur IT-systemen och rutiner fungerar. Att spela in intervjuerna har varit till stor hjälp när sammanställningen skulle göras till resultatdelen, eftersom det är svårt att anteckna allt som sägs under 30 minuter.

Det negativa med intervjuer har dock varit att få tid med personer som kan ställa upp och svara på frågorna. När intervjuerna gjordes tog dock respondenterna sig tid och hjälpte till att svara på frågorna.

Metoden med telefonintervju var ny och en del misstag gjordes därför. Dessa kan vara svåra att åtgärda i efterhand utan att behöva ta kontakt med respondenterna för en uppföljande intervju. Eftersom det finns en tidsram för arbetet har inte alla misstag kunnat åtgärdas. De flesta misstagen upptäcktes först under analysdelen när svaren från respondenterna skulle analyseras mer detaljerat.

I flera fall har inte tillräckligt med följdfrågor ställts medan intervjuerna gjorts, och i vissa fall har inte allt tänkts igenom innan sammanfattningen skickats tillbaka till respondenterna för verifiering. Under följer ett exempel på frågan om säkerhetsrutiner till IT-systemens användare:

”Nyanställda får alltid utbildning och information om säkerhet. Utbildningar sker även fortlöpande. Respondenten säger att de har uppföljning i vissa moduler och tillägger att det sker beroroende på om det är lättarbetat eller inte.”

Här borde följdfrågor ställts vad som menas med att det är lättarbetat och vad som menas med moduler. Detta kan tolkas på flera olika sätt.

Människor pratar på olika sätt och det hade då varit bra att sammanfatta intervjuerna i termer som är mer precisa för att undvika feltolkningar. En av respondenterna använder ordet reglemente.

”Det finns även regionalt reglemente”

I sammanfattningen hade meningen hade kunnat bytas ut till ”Det finns regionala regler”. Om det varit en feltolkning skulle respondenter påpekat det. Genom att ersätta ordet till något som är mer exakt blir analysen säkrare.

8.1.2 Validering
Respondenterna som har blivit intervjuade har en god insikt i patientjournalsystemen och flera av dem arbetar med det dagligen. De bör därför ha gett en trovärdig bild på situationen. Respondenternas svar har analyserats och använts för att validera på vilket sätt som patientjournalsystemen följer PbD. Tolkningarna av svaren har validerats genom att de mailats till respondenterna.

De två patientjournalsystemen som analyserats har en stor del på marknaden. Patientjournalsystemen är de två största i Sverige där de har 27,6% respektive 25,8% av alla användare (Jerlvall & Pehrsson, 2012).

Studien visar resultatet från patientjournalsystem som har över hälften av användarna i Sverige. Detta ger en bra översikt på hur det ser ut i stora delar av landet. Dock har studien enbart gjorts i två landsting, och det kan därför variera en del på rutiner och implementationen av IT-systemen. Det är därför svårt att avgöra om situationen är detsamma i de övriga landstingen i Sverige på de punkterna.

Gällande direktåtkomst till sin egen journal är det för närvarande endast Landsting B som erbjuder den tjänsten. Det finns dock pågående projekt som innebär att tjänsten ska föras in på nationell nivå (CeHis, 2013).

8.1.3 Etiska aspekter
Vårdgivarna kan tillgodogöra sig mer information än de behöver eftersom det inte går att veta i förväg vilken information de behöver. Om patientjournalsystemen istället blir mer begränsade kan vårdgivarna gå miste om viktig information som behövs för att ge patienten bästa vården. Det blir ett stort integritetsproblem eftersom med för mycket information kan integriteten bli lidande, för lite information kan vården bli lidande istället.

IT-system i hälso- och sjukvården som inte uppfyller krav som ställs på integritet, kan leda till att patientdata läcker ut. Patienter som känner att det finns säkerhetsbrister inom hälso- och sjukvården kan välja att avstå eller inte ange all information eftersom de är rädda för att informationen ska komma ut till exempelvis arbetsgivare. Informationen som de exkluderar kan vara avgörande för att de ska få en god och säker vård.

8.1.4 Samhällsnytta
Studien kan användas av ansvariga inom landstingen, och av utvecklarna av patientjournalsystemen för att hitta brister, eller utveckla funktioner, om det är något i PbD filosofin som de tycker skulle förbättra integriteten i deras IT-system.

Studien kan även läsas av medborgare som är intresserade av hur personuppgifter och information om dem behandlas och skyddas.

8.1.5 Framtida arbeten
Denna studie har enbart gjort en övergripande analys hur PbD används i patientjournalsystem för att skydda patientens integritet. Ytterligare studier skulle kunna göras genom att intervjua vårdpersonal som använder patientjournalsystemet för att få deras bild på situationen eftersom de använder det dagligen. Det var även på flera punkter som patientjournalsystemen var under utveckling. Där skulle någon typ av uppföljning göras för att se om det blivit av. Säkerhetsrutinerna till IT-systemens användare är olika på förvaltningarna så det skulle kunna göras en analys om hur det fungerar ute på de olika

förvaltningarna. Även studier i fler landsting för att kontrollera om situationen är likartad i hela landet.

Referenser

Berndtsson, M. Hansson, J. Olsson, B, Lundell, B. (2008) *Thesis Projects A Guide for students in Computer Science and Information System*. Second edition. Springer.

Cavoukian, A. (2011) *Privacy By Design The 7 foundational principles*. Tillgänglig på internet:
http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf
[Hämtad Feburari 23, 2013]

CeHis. (2013). *Journal på nätet*. Tillgänglig på internet:
http://www.cehis.se/invanartjanster/journal_pa_natet/
[Hämtad Juni 05, 2013]

Fineberg, A. Jeselon, P. (2011) *A foundational framework for a PbB – PIA*.
Tillgänglig på internet:
http://privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf
[Hämtad Feburari 23, 2013]

Fischer-Hübner, S. (2011) *Transparency Enhancing Tools & HCI for Policy Display and Informed Consent*. Privacy, Accountability, Trust – Challenges and Opportunities: ENISA Report. European Network and Information Security Agency, Technical Competence Department.

Datainspektionen. (2013) *Inbyggd integritet*. Tillgänglig på internet:
http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/
[Hämtad Feburari 23, 2013]

Gunter, T. Terry, N. (2005). *The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions*.
Journal of Medical Internet Research. Vol 7. No 1.

Jerlvall, L. Pehrsson, T. (2012) *eHälsa i landstingen*. Tillgänglig på internet:
http://www.cehis.se/images/uploads/dokumentarkiv/eHalsa_i_landstingen_SLIT_2012_rapport_utan_bilaga_120920.pdf
[Hämtad Juni 05, 2013]

SFS 1998:204. *Personuppgiftslag*.
Stockholm: Justitiedepartementet.

SFS 2008:355. *Patientdatalag*.
Socialdepartementet.

SIS. (2003) *SIS Handbok 550. Terminologi för informationssäkerhet*.
SIS Förlag AB. Stockholm.

Socialstyrelsen. (2004) *Patientsäkerhet vid elektronisk vårddokumentation*.
Rapport från verksamhetstillsyn 2003 i ett sjukvårdsdistrikt inom norra regionen. Artikelnr: 2004-109-11.

Vårdguiden. (2012) *Så hanteras dina personuppgifter*. Tillgänglig på internet: http://www.vardguiden.se/Sa-funkar-det/Lagar--rattigheter/Lagar-i-halso--och-sjukvard/Sa-hanteras-dina-personuppgifter/
[Hämtad Feburari 23, 2013]

Van Lieshout, M. Kool, L. Van Schoonhoven, B. de Jonge, M. (2011) *Privacy by Design: an alternative to existing practice in safeguarding privacy*.
Emerald Group Publishing Limited, info, Vol. 13 Iss: 6, pp.55 – 68.

Fetter, M. (2009) *Electronic Health Records and Privacy Issues in Mental Health Nursing*. Jun2009, Vol. 30 Issue 6, p408-409. 2p. Issn: 01612840

Åhlfeldt, R-M. Söderström, E. (2007) *Information Security Problems and Needs in a Distributed Healthcare Domain–A Case Study*.
Proceedings of The Twelfth International Symposium on Health Information Management Research (iSHIMR 2007).

Bilaga A - Frågor

Inledning:
Skulle ni vilja presentera er?
– Vad har ni för roll på företaget?
– Hur länge har ni varit anställd?
– Vad har ni för utbildning?

Minimera mängden personuppgifter
Hur gör ni för att minimera mängden personuppgifter som samlas in i era system?
– Hur fastställer ni vilka personuppgifter som verkligen krävs för att tillgodose era ändamål?
– Hanteras alla personuppgifter likadant? Finns det vissa personuppgifter som är extra känsliga som hanteras mer försiktigt?
– Vilka rutiner finns för att periodiskt kontrollera att datainsamling är lämpliga och relevanta och inte överdrivet omfattande i förhållande till dess ändamål?

Vilka uppgifter används i journalsystemen för att identifiera patienter (t ex personnummer, indirekt)?
-Har ni, eller skulle det vara möjligt att använda pseudonymer?

Ges patienterna möjlighet att begränsa behandling utav personuppgifterna i andra system? (Om personuppgifterna används i andra system).
- Om ja, när erbjuds denna möjlighet?
- Om nej, varför inte?

Begränsa åtkomsten till uppgifterna
Hur begränsar ni så att anställda inte kan ta del utav sådant som inte är relaterat till deras arbetsuppgifter?
– Hur hindras användare att komma åt "fel" information? D.v.s. personuppgifter som inte krävs för att lösa den aktuella arbetsuppgiften, såsom andra personers personuppgifter.
– Har era användare alltid tillgång till journaler eller enbart då de ska arbeta med dem?

Vad har ni för åtgärder för att inte systemadministratörer ska kunna läsa lagrade personuppgifter när de arbetar (t.ex. undvik med kryptering)?

Skydda uppgifterna
Vilken typ utav autentisering används för att komma åt patientjournalerna?

Vilken typ utav kryptering används
– I era databaser?
– När patienter ska ha tillgång till sina journaler direkt via webben?

– I kommunikationsnätverket för övrigt?
– Om kryptering används, vem har möjlighet att dekryptera informationen?

Hur hanteras säkerhetskopior utav krypterad data och eventuella krypteringsnycklar?

Berätta lite hur ni informerar patientjournalsystemens användare om rutiner och information om säkerhet
– Har ni någon säkerhetspolicy? Kan jag få ta del av den?
– Hur ofta informerar ni användarna om säkerhet och rutiner?
– Hur följer ni upp att dessa efterföljs?

Hur detaljerade är era loggar? (användare, dator, tidpunkt, vilken information användarna tagit del av)
– Hur är loggarna skyddade? (krypterade)
--- Om loggarna är krypterade, vilka har tillgång nyckel för att dekryptera loggarna?
– När tas säkerhetskopior utav loggarna?
– När och hur ofta förstörs loggdata?

Hur är data på era backuper skyddade? (t ex fysisksäkerhet, kryptering, autentisering)

Vad gör ni med hårddiskar och annan lagringsmedia när de tas ur bruk? (för att undvika t ex dumpster diving)

Finns det en beredskapsplan för att hantera en oförutsedd händelse?
-Beskriva riskhanteringsplanen för att återställa data som kan skadas / förloras genom:
– Mänskliga fel
– Datavirus
– Nätverksfel
– Hårddisk krasch
– Stöld
– Brand
– Översvämning.

Beskriv rutinerna för att upptäcka att inte någon obehörig kommer åt personuppgifter? Intrångsdetektering, loggar osv.

Låt systemen styra användaren rätt:
När uppgifter inte behövs längre. Hur ser ni till att de tas bort och hur vet ni vad ni kan ta bort?

Har ni tänkt på att utforma era användargränssnitt så det begränsar inmatning utav sådant som inte får skrivas in.
Om ja, hur har ni isf gjort det?
Om nej, varför inte?

Hur går ni tillväga för att samla in samtycke ifrån patienter?
– Vilken information görs det på och vid vilka tillfällen?

Hur informeras patienter om hur insamlad information kommer att behandlas?
--Har ni en integritetspolicy som sammanfattar hur informationen behandlas? Kan jag få ta del av den?

Om information behöver användas till rapporter, statistik eller forskning. Hur skyddas denna information ifrån att länkas till patienter? (anonymisering)

Transparens

Erbjuds patienterna möjlighet att se vad som är lagrat om dem i patientjournalsystem?
--Om ja, hur kan de ta del utav detta?
– Kan de se vilka som tagit del utav deras journal? Om ja, vid vilket tillfälle?
– Kan de se vem som skrivit in informationen?
– Kan de se vilka andra organisationer som tagit del utav informationen?
– Någon övrig information de kan ta del förutom det jag nämnt?

--Om nej, varför inte?

Kända brister

Finns det några problem ur integritetssynpunkt med era IT system som ni tycker behöver åtgärdas?