Datainspektionen informerar

Nr 4/2011

Allmänna råd

Enligt 1 § landskapslagen (2007:89) om Datainspektionen skall Datainspektionen följa den allmänna utvecklingen inom sitt verksamhetsområde och ta nödvändiga initiativ. Datainspektionen skall informera om gällande regler samt ge anvisningar och råd om behandlingen av personuppgifter.

Datainspektionens allmänna råd är inte bindande. De är rekommendationer om hur de bindande kraven avseende skydd av information i landskapslagen (2007:88) om behandling av personuppgifter inom kommunal- och landskapsförvaltningen (personuppgiftslagen) kan uppnås inom **hälso- och sjukvårdsproducenter** (Ålands hälso- och sjukvård) i offentlig regi.

Datainspektionen

den 21 december 2011

di.ax datainspektionen

Datainspektionen • Elverksgatan 10, AX-22100 Mariehamn, Åland • Besöksadress: Kvarteret iTiden
+358 (0)18 25 550 • +358 (0)457 34 320 81 • inspektion@di.ax • www.di.ax

Innehåll

1 Sammanfattning

Den registeransvariga (ÅHS) bör tänka på att

- Kartlägga hotbilden
- Sätta mätbara mål för säkerhet (Se till att ha de rätta förutsättningarna)
- Fastställa policy för säkerhet
- Skapa en fungerande organisation för säkerhet
- Skaffa den utrustning som behövs och använda den rätt (bl.a. testa säkerheten regelbundet)
- Upprätta regler och rutiner (bl.a. bestämma urval och omfattning, utforma en verkningsfull rutin samt följa upp att regler och rutiner iakttas och respekteras)
- Informera och utbilda kontinuerligt, bl.a. informera personalen och patienterna/vårdtagarna om att logguppföljning sker (registerbeskrivning)
- Genomföra kontrollerna
- Utvärdera rutinen
- Utveckla rutinen

2 Allmänt om information

Information är en tillgång som behöver skyddas. I landskapslagen (2007:88) om behandling av personuppgifter inom landskaps- och kommunalförvaltningen finns bestämmelser (5 kapitlet) om säkerhet vid behandling av personuppgifter. Syftet med personuppgiftslagen är att skydda människor mot att deras personliga integritet kränks vid behandling av personuppgifter. Säkerhet är en viktig del av skyddet för den personliga integriteten. För att få kontroll över organisationens informationstillgångar är det därför nödvändigt att säkerställa kontinuitet i verksamheten. Inför informationssäkerhetsarbetet behöver en infrastruktur upprättas.

> Personuppgifter är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

En informationssäkerhetspolicy formaliserar hur informationen säkerställs och behandlas inom organisationen. Således utgör informationssäkerhetspolicyn de riktlinjer som samtliga anställda arbetar efter för att bevara verksamhetens säkerhet. Den ska vara enkel, lättförståelig och koncentrerad. Utifrån informationssäkerhetspolicyn tas en systemsäkerhetsplan för varje enskilt IT-system fram[1].

[1] FR04-01 Informationssäkerhetspolicy- www.sitic.se

En *informationssäkerhetspolicy* beskriver VARFÖR en verksamhet skyddar sin information. Den är grunden i säkerhetsarbetet och ska vara genomarbetad och väl förankrad på alla nivåer i organisationen för att därigenom spegla verksamhetens värderingar.

Organisationens *systemsäkerhetsplan* beskriver VAD verksamheten har för avsikt att göra för att genomföra och upprätthålla informationssäkerheten. Den beskriver den säkerhetsmålsättning som gäller för aktuellt IT-system och klarlägger vilka säkerhetskrav som ska ställas utifrån aspekterna sekretess, riktighet och tillgänglighet. Det kan t.ex. vara riktlinjer för incidenthanteringen inom organisationen.

Anvisningarna ska på en funktionell nivå ange vilka skyddsåtgärder som ska införas. Anvisningarna beskriver PÅ VILKET SÄTT skyddet ska införas.

IT-säkerhetsinstruktioner beskriver exakt hur verksamheten kommer att uppnå de krav som den överordnade informationssäkerhetspolicyn och systemsäkerhetsplanerna förutsätter. Instruktionerna ges för specifika system eller åtgärder, t.ex. incidenthanteringen. Där beskrivs det HUR OCH AV VEM t.ex. incidenthanteringen skall införas och följas upp.

3 Informationssäkerhet

Informationssäkerhet är en viktig del av skyddet för den personliga integriteten. Enligt landskapslagen om behandling av personuppgifter inom landskaps- och kommunalförvaltningen skall den registeransvariga[2] se till att personuppgifter som behandlas i verksamheten skyddas genom tekniska och organisatoriska åtgärder. Nivån på säkerheten ska anpassas till

- vilka integritetsrisker behandlingen medför,
- hur känsliga de behandlade personuppgifterna är,
- vilka tekniska möjligheter som finns, och vad det kostar att genomföra åtgärderna

[2] Registeransvarig är normalt en juridisk person (myndighet, förening, affärsverk etc.) som behandlar personuppgifter och bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till. Det är således inte chefen eller någon ansvarig som är registeransvarig.

4 Organisation inom Ålands hälso- och sjukvård

4.1 Allmänt

Verksamheten inom hälso- och sjukvården förutsätter att det finns en säkerhetspolicy då stora mängder känsliga personuppgifter[3] hanteras. I en sådan policy redovisas organisationens säkerhetsstrategi, ansvarsfördelning och övergripande mål för säkerheten. För att säkerställa att riktlinjerna och reglerna i säkerhetspolicyn efterföljs bör kontroller genomföras. Det bör också finnas rutiner för att rapportera och följa upp incidenter. Arbetsrutiner och arbetsuppgifter bör utformas så att det blir möjligt för personalen att tänka säkerhetsmedvetet. Alla som har tillgång till personuppgifter bör få lämplig utbildning. Personalen bör informeras om vikten av att följa säkerhetsrutinerna. Loggen får dock inte användas för att övervaka att personalen uppfyller sina arbetsförpliktelser rent allmänt. Ändamålet med loggdata är rimligen att skydda patienternas/vårdtagarnas integritet.[4]

4.2 Ansvar för hälso- och sjukvården vid verksamhetsenheterna.

Varje verksamhetsenhet inom Ålands hälso- och sjukvård (i fortsättningen kallad ÅHS) leds av en klinik- eller enhetschef. De verksamhetsenheter vid ÅHS som bedriver hälso- och sjukvård ska ha en läkare eller tandläkare som är medicinskt ansvarig vid enheten. I det fall att klinikchefen inte är läkare ska den medicinskt ansvariga läkaren fungera som rådgivare till klinikchefen.

I landskapslag om hälso- och sjukvård (LR:s framställning FR 28/2010-2011/ LT:s beslut om antagande LTB 56/2011)[5] är det den medicinskt ansvariga läkaren som ansvarar för inledande och avslutande av en patients vård. Läkaren kan delegera beslutsfattandet till en annan legitimerad yrkesutbildad person.

I samma lag konstateras att ÅHS, som enda huvudman för den offentliga hälso- och sjukvården i landskapet, har sammanhållen journalföring.

[3] Känsliga uppgifter definieras i LL om behandling av personuppgifter som uppgifter som avslöjar ras och etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och även uppgifter som rör hälsa eller sexualliv.

[4] 9 § lagen om integritetsskydd i arbetslivet (FFS 477/2001) reglerar teknisk övervakning av arbetstagarna.

[5] Ersätter landskapslagen (1993:60) om hälso- och sjukvården

4.3 Patientuppgifter

Patientuppgifter är sådana känsliga uppgifter som är sekretessbelagda enligt landskapslagen om tillämpning av lagen om patientens ställning och rättigheter. Patientuppgifter får inte lämnas ut till utomstående utan patientens skriftliga samtycke med vissa undantag.

Vidare konstateras i landskapslagen om hälso- och sjukvård att det i riket finns en lag (FFS 159/2007) om elektronisk behandling av klientuppgifter inom social- och hälsovården, som reglerar elektroniska patientuppgifters sammanförande till en nationell databas med bestämmelser om överföring, hantering, tillgänglighet m.m. av dessa uppgifter, det så kallade eArkivet. Motsvarande regelverk saknas i landskapet. ÅHS kan anslutas till det nationella patientarkivet eller ordna arkivering av och tillgång till patientuppgifter på annat sätt efter att en motsvarande landskapslag har stiftats.

I riket finns även en lag (FFS 2007/61) om elektroniska recept som enligt 2 § ska tillämpas i landskapet då ÅHS infört elektroniska recept i enlighet med lagen.

5 Hotbild

För att klarlägga vilken säkerhetsnivå som ska gälla för skyddet av organisationen, information och informationssystem är det lämpligt att göra risk- och sårbarhetsanalyser. Som underlag för hur säkerhetsåtgärderna ska utformas bör det också göras en bedömning av hur sannolikt det är att olika typer av störningar ska inträffa och vilka konsekvenser det i så fall skulle få.

6 Säkerhetsåtgärder

6.1 Fysisk säkerhet

IT-utrustning som används för att behandla personuppgifter bör ha ett gott skydd mot stöld och händelser som kan förstöra utrustningen. Rutiner bör finnas för hur portabel IT-utrustning ska användas och hur utrustningen och personuppgifterna i den ska skyddas.

6.2 Tillträdeskontroll

Det bör finnas rutiner för tillträdeskontroll för att säkerställa att enbart behörig personal får tillträde till utrymmen där det finns IT-utrustning. Behovet av att kunna göra en viss arbetsuppgift kan göras till utgångspunkt för hur en tillträdeskontroll utformas. Inom ÅHS kan det förmodligen vara lämpligt att skapa områden med olika typer av tillträdeskontroll.

6.3 Behörighetskontroll

För att hindra obehöriga från att använda IT-utrustningen och bereda sig tillgång till personuppgifter bör det finnas ett system för behörighetskontroll. Systemet bör kunna identifiera användare och bekräfta användarens identitet, exempelvis genom personliga lösenord. Andra tekniker kan också komma i fråga (engångslösenord, aktiva behörighetskort eller biometriska metoder). Systemet bör också kunna kontrollera åtkomstskyddade personuppgifter så att bara de som behöver uppgifterna för sitt arbete får tillgång till dem. Rutiner för tilldelning och kontroll av behörigheter bör införas.

6.4 Behandlingshistorik (logg)

För att kunna kontrollera vilka som har haft tillgång till personuppgifterna bör det finnas behandlingshistorik som sparas en viss tid. Hur loggen ska utformas beror på hur känsliga personuppgifterna är. Uppgifterna i en logg bildar ett personregister[6] om den innehåller anteckningar om en levande person som kan identifieras. Landskapslagen om behandling av personuppgifter förutsätter att en registerbeskrivning upprättas.

En logg ska följas upp och skyddas mot otillåtna ändringar. Normalt ska den vara så detaljerad att den kan användas för att utreda om personuppgifter har använts felaktigt eller obehörigt. Om personuppgifterna är känsliga, ska loggen visa användaridentitet, tidpunkt och vilka personuppgifter användaren har haft tillgång till. Loggen ger ett förebyggande skydd. En förutsättning är dock att användarna informeras om att all användning loggas och att loggen följs upp.

6.5 Kommunikation

Förhindra att personuppgifter förstörs, ändras eller förvanskas då de överförs via nät och skydda anslutna tjänster mot obehörig åtkomst. Skyddet ska anpassas till hur känsliga uppgifterna är. När utrustning ansluts till Internet eller annat öppet nät ska anslutningen skyddas så att obehörig trafik förhindras. Organisationens utrustning och lokala nät bör skyddas så att inga obehöriga kan komma in via det öppna nätet. Om uppgifter enbart får lämnas ut till identifierade användare ska mottagarens identitet säkerställas. Känsliga personuppgifter får endast lämnas ut via öppna nät till identifierade användare vars identitet är säkerställd med en teknisk funktion som asymmetrisk kryptering (t.ex. e-legitimation), engångslösenord eller motsvarande. Dessutom ska känsliga personuppgifter vara krypterade vid överföring. Överväg också vilka åtgärder (och eventuell policy) som behövs för säker användning av Internet och e-post.

[6] Gäller varje strukturerad samling av personuppgifter som är tillgängliga enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

6.6 Åtgärder mot förlust av information

För att förhindra förlust av personuppgifter ska det finnas rutiner för säkerhetskopiering. För att säkerhetskopieringen ska fungera bör

- säkerhetskopior tas tillräckligt ofta
- regelbundna försök göras med att återskapa säkerhetskopian
- förvara kopian skyddad

6.7 Skydd mot skadliga program

För att upptäcka och skydda systemet mot skadliga program bör åtgärder vidtas.

6.8 Utplåning

När fasta eller löstagbara lagringsmedier som innehåller personuppgifter inte längre ska användas för sitt ändamål, bör medierna förstöras eller raderas på ett sådant sätt att uppgifterna inte kan återskapas. Lagringstiden för loggdata är beroende av loggens användningsändamål. Ändamålet är att skydda de registrerades integritet varför loggdata bör förvaras så länge som den registrerade kan framföra straffrättsliga krav på den som behandlar eller har åtkomst till personuppgifterna. Åtalsrätten till lagstridig behandling av personuppgifter och registerintrång är två år och en motsvarande lagringstid är att rekommendera såvida inte grunden till att bevara uppgiften förlorat sin betydelse. Lika viktigt är det att utplåna loggdata på ett säkert sätt.

6.9 Reparation och service

Bör utföras på ett sådant sätt att personuppgifter inte blir tillgängliga för obehöriga. Ingå därför avtal med utomstående serviceföretag som ska reparera eller utföra service på IT-utrustningen. Anpassa avtalet till hur känsliga personuppgifterna är som finns i systemet. Avtalet kan också innehålla bestämmelser om vilka säkerhetsrutiner som ska tillämpas i samband med servicen. Om service utförs på distans ska servicepersonalen identifieras på ett säkert sätt och endast ha tillgång till utrustningen under själva servicetillfället.[7]

[7] Ur den svenska Datainspektionens allmänna råd, Säkerhet för personuppgifter www.datainspektionen.se Krisberedskapsmyndighetens rekommendationer Basnivå för informationssäkerhet (BITS). www.krisberedskapsmyndigheten.se samt svensk standard Ledningssystem för informationssäkerhet - Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 17799:2 005) och krav (SS-ISO/IEC 27001:2 006). www.sis.se

7 Personuppgifternas art

För att kunna informera de registrerade om förekomsten av de register de finns upptagna i innehåller 5 § och 10 § landskapslagen om behandling av personuppgifter allmänna bestämmelser om den registeransvariga myndighetens skyldighet att upprätta registerbeskrivningar. En registerbeskrivning ska bland annat innehålla ändamålet med behandlingen av personuppgifter, en beskrivning av de uppgifter eller kategorier av uppgifter som behandlas om den registrerade och en allmän beskrivning av de åtgärder som har vidtagits för att trygga säkerheten i behandlingen.

Journalhandlingar bildar ett personregister. Registeransvarig är enligt landskapslagen om behandling av personuppgifter ”den myndighet som ensam eller tillsammans med andra bestämmer ändamålen med och behandlingen av personuppgifter”, d.v.s. Ålands hälso- och sjukvård. Enligt rikets personuppgiftslag är en registeransvarig ”en eller flera personer, sammanslutningar, inrättningar eller stiftelser för vilkas bruk ett personregister inrättas och vilka har rätt att förfoga över registret eller vilka lag ålagts skyldighet att föra register”, d.v.s. en verksamhetsenhet för hälso- och sjukvården eller en yrkesutbildad person inom hälso- och sjukvården som självständigt utövar sitt yrke.

Enligt 9 § social- och hälsovårdsministeriets förordning om journalhandlingar är det verksamhetsenheterna för hälso- och sjukvård eller de yrkesutbildade personer inom hälso- och sjukvården som självständigt utövar sitt yrke som ska föra en patientjournal över varje patient i fortlöpande och kronologisk form”.

För förvaringen av journalhandlingar och annat material som gäller vården ansvarar i regel den verksamhetsenhet för hälso- och sjukvård eller den självständiga yrkesutövare inom hälso- och sjukvården inom vars verksamhet handlingarna och materialet uppkommit.

Patienten har med vissa undantag rätt till insyn i vilka uppgifter om henne eller honom som antecknats i journalhandlingarna. Patienten ska utan onödigt dröjsmål ges tillfälle att ta del av uppgifterna i journalhandlingarna eller på begäran lämnas uppgifterna skriftligen.

För vården ska en vård- och rehabiliteringsplan göras upp på det sätt som bestäms i lagen om patientens ställning och rättigheter, vilken tillämpas som blankettlag i landskapet.

8 Sekretess- och användarförbindelse

För att trygga integritetsskyddet är det viktigt att sörja för att de personuppgifter som behandlas skyddas i alla skeden av behandlingen. Mera om skyddsplikten finns i 18 och 19 § § landskapslagen om behandling av personuppgifter. För personuppgifter som behandlas med ADB består skyddet av bl.a. de olika egenskaperna hos olika datasystem, program, utrustningar, datanät och på vilket sätt de används, eventuella användarrättigheter samt övervakningen av användningen och i hur verksamheten är organiserad.

Särskild vikt bör fästas vid skyddet av sekretessbelagda och känsliga uppgifter. Uppgifter som gäller hälsotillståndet är sådana känsliga personuppgifter som avses i 3 kapitlet landskapslag om behandling av personuppgifter. Patientuppgifter är också enligt 13 § lagen om patientens ställning och rättigheter sådana uppgifter som bör hållas hemliga.

Även om datasystemet är säkert är det avgörande att personalen känner till kravet på dataskyddet, kan använda systemen samt följer myndighetens/sjukvårdsproducentens anvisningar. Personalen bör därför instrueras och utbildas. Vidare bör användningen av systemen och behandlingen av personuppgifter följas upp. I syfte att särskilt betona kravet på dataskydd och sekretess kan en särskild sekretess- och användarförbindelse med personalen upprättas. På www.tietosuoja.fi finns en mall.

9 Gällande lagstiftning

9.1 Allmänt

Rent allmänt kan sägas, såvida verksamheten vid Ålands hälso- och sjukvård inte styrs av någon speciallag så gäller landskapslagen om behandling av personuppgifter inom landskaps- och kommunalförvaltningen och landskapslagen (2007:88) om allmänna handlingars offentlighet vid behandling av personuppgifter. Till den del Ålands hälso- och sjukvård utför uppgifter och därmed hanterar personuppgifter som enligt 27 § självstyrelselagen hör till rikets lagstiftningsbehörighet tillämpas rikets personuppgiftslag (FFS 523/1999).

Datainspektionen anser att den i grundlagen garanterade rättigheten som gäller skyddet av privatlivet väger tyngre än övriga grundläggande rättigheter som gäller offentlighet. Riksdagens biträdande justitieombudsman har i ett fall ansett integritetsskyddet vara en mer vägande grundläggande rättighet än offentlighet och yttrandefrihet. Denna slutsats kom justitieombudsmannen till trots att den enskilda i offentligheten redogjort för sitt sjukdomstillstånd[8].

[8] Beslut 17.5.2010/Dnr 4510/4/09 gällande landskapsregeringens publicering av protokoll på webbsidan.

9.2 Lagstiftningsbehörigheten

Enligt 18 § 12 p. självstyrelselagen (1991:71) har landskapet behörighet i fråga om hälso- och sjukvård, med de undantag som stadgas i 27 § 24, 29 och 30 punkterna. Till rikets behörighet hör enligt 27 § 24 p. bestämmelser om administrativa ingrepp i den personliga friheten, enligt 27 § 29 p. bestämmelser om smittsamma sjukdomar hos människor, kastrering och sterilisering, avbrytande av havandeskap, konstbefruktning och rättsmedicinska undersökningar samt enligt 27 § 30 p. bestämmelser om behörigheten att vara verksam inom hälso- och sjukvården, apoteksväsendet, mediciner och produkter av läkemedelstyp, narkotiska ämnen samt framställning av gifter och fastställande av deras användningsändamål.

Ålands hälso- och sjukvårds delaktighet i bland annat rikstäckande register för elektroniska recept (FFS 617/2007) samt elektronisk behandling inom social- och hälsovården (FFS 159/2007) förutsätter åländsk lagstiftning, möjligen genom kompletterande överenskommelseförordningar. Av landskapslag om hälso- och sjukvård (LR:s framställning FR 28/2010-2011/ LT:s beslut om antagande LTB 56/2011 kommer de områden som landskapsregeringen avser att reglera på förordningsnivå att vara screening (28 §), rådgivning för gravida och barn under läropliktsåldern (29 §), skolhälsovård (30 §), studerandehälsovård (31 §), mun- och tandvård (40 §), medicinsk rehabilitering (43 §) samt prehospital akutsjukvård (45 §).

Handräckning till polisen och tullmyndigheterna sker utan lagstöd genom en särskild överenskommelse mellan ÅHS, tullmyndigheten och polisen. I landskapslag om hälso- och sjukvård (LR:s framställning FR 28/2010-2011/ LT:s beslut om antagande LTB 56/2011) finns en bestämmelse som motsvarar den tidigare gällande folkhälsolagen kompletterad så att även tullmyndigheterna kan få handräckning för utförande av kliniska undersökningar av levande personer. Enligt tullagen har tullmyndigheten rätt att hejda en person och företa kroppsbesiktning om personen på sannolika skäl misstänks för brott för vilket det strängaste straffet är fängelse i minst sex månader.

9.3 Lagstiftning

Åtminstone följande lagstiftning gällande hantering av personuppgifter inom hälso- och sjukvården är tillämplig, nämligen:

- Landskapslag (2007:88) om behandling av personuppgifter inom landskaps- och kommunalförvaltningen (klassificering av personuppgifter, registerbeskrivningar[9])
- Personuppgiftslagen (FFS 523/1999)[10]
- Landskapslagen (1977:72) om allmänna handlingars offentlighet
- Arkivlag (2004:13)

[9] Dataombudsmannens modell nr 1/2001 (15.8.2001) för analys av behandlingen av personuppgifter/registerfunktionerna för personuppgifter www.tietosuoja.fi

[10] Till den del ÅHS utför uppgifter och därmed hanterar personuppgifter som enligt 27 § självstyrelselagen hör till rikets lagstiftningsbehörighet tillämpas rikslagstiftningen.

- Landskapslag (1993:61) om tillämpning i landskapet Åland av lagen om patientens ställning och rättigheter (FFS 785/1992) (Patientlagen)
- Social- och hälsovårdsministeriets förordning om journalhandlingar (FFS 298/2009)[11]
- Republikens Presidents Förordning (2005:64) om vissa förvaltningsuppgifter inom hälso- och sjukvården i landskapet Åland (FFS 803/2005)
- Lag om integritetsskydd i arbetslivet (FFS 759/2004)
- Lag om dataskydd vid elektronisk kommunikation (FFS 516/2004)
- Lag om yrkesutbildade personer inom hälso- och sjukvården (FFS 559/1994)
- Förordning om yrkesutbildade personer inom hälso- och sjukvården (FFS 564/1994)
- Landskapslag om hälso- och sjukvård (LR:s framställning FR 28/2010-2011/ LT:s beslut om antagande LTB 56/2011)[12]
- Landskapslag (2007:23) om grunderna för avgifter för Ålands hälso- och sjukvård[13]

Rikslagstiftningen finns på http:www.finlex.fi/uppdaterad lagstiftning.
Landskapslagstiftningen finns på http://www.regeringen.ax/lag.pbs

[11] Tillämpas i landskapet med stöd av 1§ i blankettlag (1993:61) om tillämpning i landskapet Åland av lagen om patientens ställning och rättigheter. Notera att landskapsregeringen, och inte Datainspektionen, har tillsynsansvar inom landskapets behörighetsområden enligt blankettlagens 3 §, jfr även med 2 § 3 och 5 punkten.
[12] Ersätter landskapslagen (1993:60) om hälso- och sjukvården
[13] Genom 2011:82 ändras 4 § 1 mom. och 5 § 2 och 3 mom., sådant 4 § 1 mom. lyder i LL 2009:67, fogas till 5 § ett nytt 5 mom., upphävs 6 § 4 mom. 2,3 och 6 punkten LL (2009:23) om grunderna för avgifterna till ÅHS