Alþingi
Heilbrigðisnefnd
150 REYKJAVÍK

Persónuvernd

Rauðarárstíg 10 105 Reykjavík
sími: 510 9600 bréfasími: 510 9606
netfang: postur@personuvernd.is
veffang: personuvernd.is

Reykjavík, 18. ágúst 2008
Tilvísun: 2008060445 ÞS/--

Efni: Umsögn um frumvarp til laga um sjúkraskrár

Persónuvernd vísar til bréfs heilbrigðisnefndar Alþingis, dags. 4. júní 2008, þar sem óskað er umsagnar um frumvarp til laga um sjúkraskrár (þskj. 1086, 635. mál á 135. löggjafarþingi). Umsagnarinnar var óskað fyrir 1. júlí 2008, en með bréfi, dags. 18. s.á., var tilkynnt að vegna anna Persónuverndar yrði ekki unnt að skila umsögninni innan þess frests. Hún yrði hins vegar send heilbrigðisnefnd í vikunni 6.–12. júlí.

I.

Með frumvarpinu er lagt til að sett verði heildarlög sem fjalli gagngert um sjúkraskrár, þ. á m. skyldu til færslu þeirra, hvaða upplýsingar þær skuli hafa að geyma og aðgang heilbrigðisstarfsfólks og sjúklinga sjálfra að skránum. Slík heildarlög hafa ekki áður verið sett, en í reglugerð er hins vegar að finna ákvæði sem fjalla um helstu atriði varðandi færslu sjúkraskráa, nánar tiltekið reglugerð nr. 227/1991 um sjúkraskrár og skýrslugerð varðandi heilbrigðismál. Sú reglugerð sækir nú stoð í 6. mgr. 14. gr. laga um réttindi sjúklinga. Það ákvæði er í IV. kafla laganna sem hefur að geyma nokkrar meginreglur um varðveislu sjúkraskráa og aðgang heilbrigðisstarfsfólks að þeim, sem og reglur um rétt sjúklings til aðgangs að eigin sjúkraskrá.

Talsverðar breytingar munu verða frá ríkjandi réttarástandi verði frumvarpið að lögum óbreytt. Þau lög munu þá hafa að geyma ítarleg ákvæði um rafrænar sjúkraskrár, en ákvæðum um slíkar skrár er ekki til að dreifa í gildandi rétti, sbr. þó 4. mgr. 5. gr. reglugerðar nr. 227/1991 þar sem segir að sjúkraskrár sé heimilt að tölvufæra enda sé þess gætt við tölvufærsluna að um er að ræða upplýsingar um einkahagi sjúklings sem ekki eru ætlaðar öðrum til skoðunar.

Meðal helstu atriða frumvarpsins eru:

1. Að sjúkraskrár skuli færðar í rafrænu formi að því marki sem unnt er, sbr. 2. mgr. 4. gr.

2. Að einungis heilbrigðisstarfsmenn og aðrir starfsmenn og nemar í starfsnámi í heilbrigðisvísindum, sem undirgengist hafa sambærilega trúnaðar- og þagnarskyldu og

heilbrigðisstarfsmenn, megi færa sjúkraskráruppplýsingar í sjúkraskrár, sbr. 1. mgr. 5. gr.

3. Að sjúklingur geti sjálfur ákveðið að einungis tiltekinn eða tilteknir heilbrigðisstarfsmenn hafi aðgang að sjúkraskrá hans en skuli þá upplýstur um að slíkt geti, eftir atvikum, jafngilt því að meðferð sé hafnað, sbr. 1. mgr. 7. gr.

4. Að sjúklingur skuli eiga rétt á að færðar séu leiðréttingar í sjúkraskrá og að ágreiningi í tengslum við slíkt megi skjóta til landlæknis, sbr. 2. mgr. 7. gr.

5. Að þegar sjúklingur færi sig frá einni heilsugæslustöð til annarrar skuli vista afrit sjúkraskrár hans í því sjúkraskrárkerfi sem notað er á þeirri stöð sem hann flyst til, sbr. 1. mgr. 10. gr.

6. Að heilbrigðisstarfsmenn, sem koma að meðferð sjúklings og þurfa á sjúkraskráruppplýsingum að halda vegna starfa sinna, skuli hafa aðgang að sjúkraskrá hans, með þeim takmörkunum sem leiði af ákvæðum frumvarpsins og reglna settra samkvæmt þeim. Umsjónaraðili sjúkraskráa (þ.e. læknir eða annar heilbrigðisstarfsmaður sem heilbrigðisstofnun eða starfsstofa heilbrigðisstarfsmanna hefur falið að hafa eftirlit með því að meðferð sjúkraskráruppplýsinga samrýmist lögum, sbr. 13. tölul. 3. gr.) geti veitt öðrum starfsmönnum og nemum í starfsnámi í heilbrigðisvísindum, sem undirgengist hafa sambærilega trúnaðar- og þagnarskyldu og heilbrigðisstarfsmenn og koma að meðferð sjúklings, heimild til aðgangs að sjúkraskrá að því marki sem nauðsynlegt er vegna starfa þeirra í þágu sjúklings, sbr. 1. mgr. 13. gr.

7. Að aðgang að sérstaklega viðkvæmum sjúkraskráruppplýsingum skuli að jafnaði takmarka við starfsmenn þeirrar einingar eða deildar heilbrigðisstofnunar eða starfsstofu heilbrigðisstarfsmanna þar sem meðferð er veitt. Aðgangur annarra heilbrigðisstarfsmanna að upplýsingunum sé þá óheimill án samþykkis sjúklings, sbr. 2. mgr. 13. gr.

8. Að sjúklingur skuli hafa aðgang að eigin sjúkraskrá með nánar tilteknum takmörkunum, sbr. 14. gr.

9. Að sjúklingur eigi rétt á að fá að vita frá umsjónaraðila sjúkraskrár hverjir hafi aflað upplýsinga úr sjúkraskrá hans, m.a. með samtengingu sjúkraskrárkerfa (sbr. V. kafla frumvarpsins), hvar og hvenær upplýsinga var aflað og í hvaða tilgangi, sbr. 4. mgr. 14. gr.

10. Að nánir aðstandendur látins einstaklings skuli hafa aðgang að sjúkraskrá hans að nánar tilteknum skilyrðum fullnægðum, þ. á m. heimild landlæknis, ef þeir telja að eitthvað hafi farið úrskeiðis við meðferð. Aðgangur að sjúkraskrá látins einstaklings sé í öðrum tilvikum háður því að hann hafi samþykkt aðganginn í lifanda lífi, að fyrir liggi sérstök lagaheimild eða dómsúrskurður, sbr. 15. gr.

11. Að heilbrigðisyfirvöld, sem lögum samkvæmt hafa til umfjöllunar kvörtun eða kæru sjúklings eða umboðsmanns hans vegna meðferðar, eigi rétt til aðgangs að sjúkraskrá viðkomandi með sama hætti og sjúklingur sjálfur, sbr. 16. gr.

12. Að leyfi Persónuverndar þurfi til aðgangs að sjúkraskrá vegna vísindarannsókna á heilbrigðissviði, sbr. 17. gr.

13. Að umsjónaraðili sjúkraskrár megi veita heilbrigðisstarfsmönnum og öðrum starfsmönnum og nemum í starfsnámi í heilbrigðisvísindum, sem undirgengist hafa sambærilega trúnaðar- og þagnarskyldu og heilbrigðisstarfsmenn, aðgang að sjúkraskrám vegna gæðaþróunar og

gæðaeftirlits með heilbrigðisþjónustu og meðferð innan viðkomandi heilbrigðisstofnunar eða starfsstofu heilbrigðisstarfsmanna, sbr. 18. gr.

14. Að samtengja megi sjúkraskrárkerfi fleiri en einnar heilbrigðisstofnunar eða starfsstofu heilbrigðisstarfsmanna – eða, m.ö.o., að umsjónaraðili sjúkraskrár megi veita heilbrigðisstarfsmönnum annarra heilbrigðisstofnana eða annarra starfsstofa heilbrigðisstarfsmanna, sem ekki eiga aðild að kerfinu, beinan aðgang að sjúkraskrá. Bæði heilbrigðisstarfsmenn, sem eru eru í beinum samskiptum við sjúkling vegna meðferðar, sem og eftir atvikum nemar í starfsnámi í heilbrigðisvísindum, sem undirgengist hafa sambærilega þagnarskyldu og þeir, megi þá afla upplýsinga úr sjúkraskránni. Sjúklingur eða umboðsmaður hans geti bannað miðlun sjúkraskrárupplýsinga með samtengingu sjúkraskrárkerfa en skuli þá upplýstur um að slíkt geti haft neikvæð áhrif á meðferð. Um öryggi persónuupplýsinga fari samkvæmt lögum um persónuvernd og meðferð persónuupplýsinga og reglum settum með stoð í þeim, sbr. V. kafla.

15. Að heilbrigðisstofnunum og starfsstofum heilbrigðisstarfsmanna sé heimilt, með leyfi heilbrigðisráðherra, að færa og varðveita sjúkraskrár í sameiginlegu sjúkraskrárkerfi, enda sé slíkt til þess fallið að tryggja betur öryggi sjúklinga við meðferð. Ráðherra geti bundið leyfi nauðsynlegum skilyrðum. Þá skuli leyfi m.a. ávallt bundið því skilyrði að fyrir liggi staðfesting Persónuverndar á því að öryggi persónuupplýsinga í hinu sameiginlega sjúkraskrárkerfi sé tryggt. Sjúklingur eða umboðsmaður hans geti bannað að sjúkraskrárupplýsingar séu aðgengilegar, að hluta eða að öllu leyti, utan þeirrar heilbrigðisstofnunar eða starfsstofu heilbrigðisstarfsmanna þar sem þær eru skráðar, þ.e. að því marki sem það er tæknilega mögulegt. Auk þess geti sjúklingur eða umboðsmaður hans lagt bann við því að tilgreindir aðilar afli um hann sjúkraskrárupplýsinga. Skuli sjúklingur upplýstur um að takmörkun á aðgangi kunni að hafa neikvæð áhrif á meðferð, sbr. VI. kafla.

16. Ábyrgðar- og umsjónaraðilar sjúkraskrár skuli hafa virkt eftirlit með því að farið sé að lögum og hafi umsjónaraðili sjúkraskráa rétt til aðgangs að sjúkraskrám að því marki sem nauðsynlegt sé í þágu eftirlitsins. Þá hafi landlæknir eftirlit með því að farið sé að umræddum reglum, auk þess sem Persónuvernd hafi eftirlit með öryggi og vinnslu persónuupplýsinga í sjúkraskrám í samræmi við ákvæði laga um persónuvernd og meðferð persónuupplýsinga. Leiði eftirlit í ljós að verulegar líkur séu á að brotið hafi verið gegn persónuverndarhagsmunum sjúklings skuli brotið kært til lögreglu, sbr. 23. gr.

II.

Af upptalningunni í I. kafla umsagnar þessarar er ljóst að umrætt frumvarp felur í sér margvísleg nýmæli. Segja má að engin þeirra ákvæða, sem þar eru talin upp, eigi sér fyrirmynd í gildandi lögum að þeim undanskildum sem nefnd eru í 2., 8. og 12. tölul. Ákvæðið, sem nefnt er í 2. tölul., og lýtur að því hverjir megi færa sjúkraskrár, á sér hliðstæðu í 2. mgr. 3. gr. og 2. mgr. 5. gr. reglugerðar nr. 227/1991 (þau ákvæði útiloka þó ekki samkvæmt orðalagi sínu að aðrir en þar eru nefndir færi sjúkraskrár). Þá eiga ákvæðin um aðgang sjúklings að eigin sjúkraskrá, sem vikið er að í 8. tölul., sér fyrirmynd í 2.–5. mgr. 14. gr. laga nr. 74/1997 um réttindi sjúklinga, auk þess sem ákvæðin, sem vikið er að í 12. tölul., hafa að geyma sömu reglu og 3. mgr. 15. gr. sömu laga, þ.e. að leyfi Persónuverndar þurfi til aðgangs að sjúkraskrám í þágu vísindarannsókna á heilbrigðissviði.

Meðal nýmæla frumvarpsins má nefna ákvæði um að nemar í heilbrigðisvísindum geti skoðað sjúkraskrá eftir því sem nauðsynlegt getur talist og að nánir ættingjar hafi aðgang að sjúkraskrá látins sjúklings í ákveðnum tilvikum, sbr. 6. og 10. tölul. I. kafla umsagnar þessarar. Þá er það m.a. nýmæli að sérstaklega sé mælt fyrir um heimild til aðgangs að sjúkraskrám í þágu

gæðaeftirlits, sbr. 13. tölul. sama kafla. Í framkvæmd hefur Persónuvernd, m.a. í ljósi 8. tölul. 1. mgr. 9. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga, gert þann greinarmun á slíkum aðgangi og aðgangi vegna vísindarannsókna að ekki þurfi leyfi samkvæmt framangreindu ákvæði laga um réttindi sjúklinga vegna fyrrnefnda aðgangsins. Er það fallið til skýringar að þetta komi sérstaklega fram í lögum.

Veigamesta breytingin frá gildandi rétti, sem umrædd nýmæli hafa í för með sér, verði frumvarpið að lögum, er að heilbrigðisstofnunum og starfsstofum heilbrigðisstarfsmanna verður heimilað að samtengja eða taka upp sameiginleg, rafræn sjúkraskrárkerfi að tilteknum skilyrðum fullnægðum, sbr. 14. og 15. tölul. I. kafla umsagnar þessarar. Gildandi lög fela í sér veigamiklar takmarkanir á því, sbr. einkum 1. mgr. 14. gr. laga nr. 74/1997 þar sem segir að sjúkraskrá skuli varðveita á heilbrigðisstofnun þar sem hún er færð eða hjá lækni eða öðrum heilbrigðisstarfsmanni sem hana færir á eigin starfsstofu.

Ákvæði frumvarpsins bera með sér að gert er ráð fyrir að ýmsir heilbrigðisstarfsmenn muni geta haft víðtækan aðgang að rafrænum sjúkraskrám. Það feli í sér að aðgangur – þ.e. í þeirri merkingu *að unnt sé að nálgast tilteknar upplýsingar þó svo að það sé ekki endilega heimilt* – afmarkist þá ekki við upplýsingar um þá sjúklinga sem viðkomandi heilbrigðisstarfsmaður hefur til meðferðar hverju sinni heldur geti hann einnig nálgast upplýsingar um aðra sjúklinga. Honum sé hins vegar aðeins heimilt að nálgast tilteknar upplýsingar sé það *nauðsynlegt vegna meðferðar* – með vissum undantekningum þó, þ.e. þegar upplýsinga er aflað vegna gæðaeftirlits eða vísindarannsókna, sbr. 12. og 13. tölul. I. kafla umsagnar þessarar.

Það sem að framan segir um víðtækan aðgang að sjúkraskrám kemur ekki fram í ákvæðum frumvarpsins með beinum hætti. Það kemur hins vegar fram í athugasemdum greinargerðar með frumvarpinu, m.a. þeim orðum í V. hluta 5. kafla almennra athugasemda að samtenging sjúkraskrárkerfa geri það að verkum að aðgangur heilbrigðisstarfsmanna verði víðtækari og í einhverjum tilvikum víðtækari en sjúklingur geti kært sig um. Það kemur og fram í því að gert er ráð fyrir að ákveðnar upplýsingar lúti sérstökum aðgangstakmörkunum í ljósi viðkvæms eðlis þeirra og séu því aðeins aðgengilegar heilbrigðisstarfsmönnum á þeirri einingu eða deild þar sem þær voru skráðar, sbr. 7. tölul. I. kafla umsagnar þessarar.

Að auki kemur það fram í ákvæðum sem bera það með sér að eiga að vega á móti þeirri ógn sem vernd persónuupplýsinga getur stafað af hinum víðtæka aðgangi. Má hér m.a. nefna ákvæði um annars vegar sjálfsákvörðunarrétt sjúklinga og hins vegar virkt eftirlit með því að aðgangur sé ekki misnotaður. Sjálfsákvörðunarrétturinn birtist í ákvæðum um að sjúklingur geti sjálfur látið takmarka aðgang að sjúkraskráruppplýsingum sem sig varða þannig að þær verði ekki aðgengilegar nema á tilteknum stofnunum eða starfsstofum heilbrigðisstarfsmanna eða, ef svo ber undir, tilgreindum heilbrigðisstarfsmönnum, sbr. 3., 14. og 15. tölul. I. kafla umsagnar þessarar. Virkt eftirlit birtist í því – eins og ráðið verður af frumvarpinu – að til staðar sé skráning á því hvenær og hvers vegna heilbrigðisstarfsmenn opna sjúkraskrá – eða, m.ö.o., að viðhöfð sé svonefnd aðgerðaskráning (loggun).

Ekki er tekið fram í ákvæðum frumvarpsins að slík skráning skuli fara fram (sbr. þó 2. mgr. 17. gr. þar sem segir að það skuli skráð í sjúkraskrá þegar hún er skoðuð vegna vísindarannsóknar). Í lok almennra athugasemda í greinargerð er hins vegar vikið að aðgerðaskráningu. Til þess ber og að líta að virkt eftirlit, sbr. 16. tölul. I. kafla umsagnar þessarar, er útilokað án slíkrar skráningar. Að auki er hún forsenda þess að unnt sé að fara að því ákvæði frumvarpsins að sjúklingur geti fengið upplýsingar um það hverjir hafi aflað upplýsinga úr sjúkraskrá hans, sbr. 9. tölul. sama kafla. Enn má nefna að aðgerðaskráningu má telja forsendu varnaðaráhrifa þess ákvæðis að kæra skuli það til lögreglu ef verulegar líkur eru á að brotið hafi verið gegn

persónuverndarhagsmunum sjúklings, sbr. 16. tölul. I. kafla umsagnar þessarar.

III.

Af framangreindu verður ráðið að með frumvarpinu er leitast við að gæta jafnvægis milli annars vegar hagsmuna sjúklinga af friðhelgi einkalífs og hins vegar þeirra hagsmuna sem eru af því að veita bestu heilbrigðisþjónustu sem völ er á, en það felur m.a. í sér að öryggi sjúklinga sé ekki ógnað þar eð heilbrigðisstarfsfólk geti ekki nálgast nauðsynlegar upplýsingar. Í framkvæmd hefur Persónuvernd fjallað um það til hvers beri að líta í þessu sambandi, sbr. einkum ákvörðun hennar frá 19. febrúar 2007 um aðgangsheimildir að rafrænum sjúkraskrám á Landspítala (mál nr. 2005/384). Þar segir m.a.:

> „Í „upplýsingaöryggi" felast þrír grundvallarþættir: (a) Að persónuupplýsingum sé leynt gagnvart óviðkomandi, (b) að þær séu áreiðanlegar og (c) að þær séu aðgengilegar þeim sem nauðsynlega þurfa á þeim að halda. Allir þessir þættir eru mikilvægir við vernd sjúkraskrárupplýsinga, en almennt er þó talið að við notkun þeirra í heilbrigðisþjónustu vegi áreiðanleiki upplýsinga og nauðsynlegt aðgengi heilbrigðisstarfsmanna að þeim þyngst, enda er hvoru tveggja mikilvægt til að tryggja góða heilbrigðisþjónustu. Með því er þó ekki gert lítið úr mikilvægi leyndar gagnvart óviðkomandi."

Þegar litið var til þessa taldi Persónuvernd, að svo stöddu, að ekki væri ástæða til að endurskoða mat Landspítala á því hversu víðtækar aðgangsheimildir að sjúkraskrám þyrftu að vera, m.a. að læknar og hjúkrunarforstjórar skyldu hafa aðgang að öllum sjúkraskrárupplýsingum á spítalanum að undanskildum þeim sem væru sérlega viðkvæmar. Hins vegar var lögð rík áhersla á aðgerðaskráningu sem hefði m.a. að geyma rökstuðning heilbrigðisstarfsmanna fyrir aðgangi í einstökum tilvikum (s.s. með því að haka við tiltekinn reitt í tölvuviðmóti); að framangreindar upplýsingar, sem teldust sérstaklega viðkvæmar (t.d. í tengslum við geðsjúkdóma og um félagsleg vandamál), skyldu háðar sérstökum aðgangstakmörkunum; og að viðhaft skyldi reglubundið eftirlit með aðgerðaskráningu.

Persónuvernd telur ákvæði umrædds frumvarps fara að ýmsu leyti saman við þá framkvæmd stofnunarinnar sem hér er lýst.

Gerir stofnunin engar athugasemdir við þá meginnálgun frumvarpsins að aðgangur að sjúkraskrám skuli mótast af því sem nauðsynlegt er vegna öryggis sjúklinga en að m.a. virku, eftirfarandi eftirliti skuli beitt til að vega á móti þeim ógnum við vernd persónuupplýsinga sem aðgangurinn getur haft í för með sér. Hins vegar gerir stofnunin athugasemdir við eftirfarandi, einstök atriði í frumvarpinu:

1. Í 3. mgr. 1. gr. frumvarpsins segir: „Að svo miklu leyti sem ekki er mælt fyrir um á annan veg í lögum þessum gilda ákvæði laga um persónuvernd og meðferð persónuupplýsinga um sjúkraskrárupplýsingar og meðferð þeirra." Persónuvernd telur ekki ástæðu til breytinga á þessu ákvæði en bendir á að reglum frumvarpsins er ætlað að tryggja persónuvernd sjúklinga. Í ljósi þess ættu ákvæði þess aldrei að vera túlkuð á þann veg að þau leiði til lakari réttarverndar en samkvæmt lögum nr. 77/2000. Þó svo að ákvæði frumvarpsins séu ekki þannig orðuð að sérstök ástæða sé til að búast við slíkri túlkun telur Persónuvernd rétt að benda á þetta til áréttingar.

2. Í 2. mgr. 7. gr. segir m.a. að sé sýnt fram á að upplýsingar í sjúkraskrá séu bersýnilega rangar eða villandi sé heimilt með samþykki umsjónaraðila að leiðrétta þær í sjúkraskrá viðkomandi. Hafa ber í huga í þessu sambandi að sú staðreynd að skráðar hafi verið rangar eða villandi upplýsingar í sjúkraskrá getur haft gildi vegna réttarágreinings, t.d. vegna ætlaðra mistaka í heilbrigðisþjónustunni. Í ljósi þess leggur Persónuvernd til að við 2. málsl. 2. mgr. 7. gr. verði bætt við orðunum *„enda sé þess gætt að ekki glatist upplýsingar sem nauðsynlegar eru vegna*

réttarágreinings". Til að fara að slíkri reglu væri t.d. hægt að prenta út þann hluta sjúkraskrár, sem leiðrétta á, áður en hann er leiðréttur og afhenda sjúklingi þannig að hann geti notað útprentunina til að gæta hagsmuna sinna.

3. Í 1. mgr. 19. gr. segir að umsjónaraðila sjúkraskrár sé heimilt að veita heilbrigðisstarfsmönnum annarra heilbrigðisstofnana eða annarra starfsstofa heilbrigðisstarfsmanna, sem ekki eiga aðild að sjúkraskrárkerfi viðkomandi stofnunar, beinan aðgang að sjúkraskrá með samtengingu rafrænna sjúkraskrárkerfa hafi sjúklingur ekki bannað slíkan aðgang, sbr. 20. gr. Persónuvernd telur málefnaleg rök geta staðið fyrir veitingu aðgangs að rafrænum sjúkraskrárkerfum með þessum hætti. Hins vegar telur stofnunin ástæðu til að orða ákvæðið á þann veg að skýrt komi fram að slíkur beinn aðgangur, sem hér um ræðir, nái aðeins til tilgreindra starfsmanna. *Leggur því stofnunin til að á undan orðinu „heilbrigðisstarfsmanna" í 1. málsl. 1. mgr. 19. gr. verði bætt orðinu „tilgreindra".* Verður þá um leið skýrt að sá aðgangur, sem til er stofnað með samtengingu sjúkraskrárkerfa, nær aðeins til þeirra sem koma að meðferð eða veita ráðgjöf í tengslum við meðferð þeirra sjúklinga sem um ræðir.

4. Í 1. mgr. 20. gr. er lögð til regla um rétt sjúklings til að fá fram bann við miðlun upplýsinga um hann með samtengingu rafrænna sjúkraskrárkerfa. Bannið á að geta tekið til annaðhvort allra upplýsinga í rafrænu sjúkraskrárkerfi eða tiltekinna upplýsinga sem þar eru varðveittar. Þá segir að sjúklingur geti lagt bann við því að tilgreindir aðilar geti aflað upplýsinga um hann með samtengingu rafrænna sjúkraskrárkerfa. Í ákvæðinu er, hvað varðar takmörkun á aðgangi að tilteknum sjúkraskráruppplýsingum, gerður fyrirvari um að slík takmörkun sé tæknilega möguleg. Persónuvernd vekur athygli á að nú þegar er tæknilega mögulegt að varðveita tilteknar, rafrænar sjúkraskráruppplýsingar í því sem kalla má sérstökum hólfum sem þrengri aðgangur er að en ella væri. Slíkt verklag tíðkast m.a. á Landspítala. Í ljósi þess telur Persónuvernd umræddan fyrirvara óþarfan *og leggur til að eftirfarandi orð verði felld brott úr 3. málsl. 1. mgr. 20. gr.: „að því marki sem það er tæknilega mögulegt hjá viðkomandi ábyrgðaraðila sjúkraskráa".*

5. Í 2. mgr. 20. gr. segir að nýti sjúklingur rétt sinn samkvæmt fyrrnefndu ákvæði 1. mgr. sömu greinar skuli hann upplýstur um að meðferð geti orðið ómarkvissari en ella þar sem ekki sé hægt að afla heildstæðra upplýsinga um hann. Í 2. mgr. er lögð til sú regla að ákvörðun um takmörkun á aðgangi að sjúkraskrám með samtengingu sjúkraskrárkerfa skuli vera skrifleg og að heilbrigðisstarfsmaður skuli staðfesta að þessi fræðsla hafi verið veitt. Persónuvernd bendir á í þessu sambandi að í ákveðnum tilvikum kunna upplýsingar í sjúkraskrá að vera þess eðlis að takmörkun á aðgangi samkvæmt framangreindu hafi ekki neikvæð áhrif á meðferð. *Leggur stofnunin því til að innskotinu „eftir því sem við á" verði bætt við á eftir orðunum „upplýsa hann" í 1. máls. 2. mgr. 20. gr. og „jafnframt staðfestir" í 2. málsl. 3. mgr. sömu greinar.* Í þessu sambandi bendir Persónuvernd á orðalag 2. málsl. 1. mgr. 7. gr. frumvarpsins sem virðist byggjast á sömu sjónarmiðum og hér eru höfð að leiðarljósi.

6. Í 1. mgr. 22. gr. er lögð til regla um rétt sjúklings til að takmarka aðgang að sjúkraskráruppplýsingum sem vistaðar eru í sameiginlegu sjúkraskrárkerfi tveggja eða fleiri heilbrigðisstofnana. Í því felst að þær verða aðeins aðgengilegar á þeirri heilbrigðisstofnun eða starfsstofu heilbrigðisstarfsmanns þar sem þær eru færðar. Gerður er fyrirvari um að slík takmörkun á aðgangi sé tæknilega möguleg. Persónuvernd gerir hér sömu athugasemd og við 1. mgr. 20. gr., sbr. 4. tölul. hér að ofan. Leggur stofnunin því til að orðin *„að því marki sem það er tæknilega mögulegt"* verði felld brott úr 2. málsl. 1. mgr. 22. gr.

7. Í 2. mgr. 22. gr. segir að ákvörðun samkvæmt 1. mgr. sömu greinar skuli vera skrifleg og

staðfest af heilbrigðisstarfsmanni sem jafnframt staðfesti að útskýrt hafi verið fyrir sjúklingi að vegna ákvörðunar hans um takmörkun á aðgangi geti meðferð orðið ómarkvissari en ella þar sem ekki sé hægt að afla heildstæðra upplýsinga um sjúklinginn. Persónuvernd telur að í ákveðnum tilvikum kunni takmörkun á aðgangi ekki að hafa þessar afleiðingar eins og lýst er í umfjöllun um 2. mgr. 20. gr. frumvarpsins, sbr. 5. tölul. hér að ofan. *Leggur stofnunin því til að orðunum „eftir því sem við á" verði bætt við á eftir orðunum „jafnframt staðfestir" í í 2. málsl. 2. mgr. 22. gr.*

8. Að lokum leyfir Persónuvernd sér að benda á tvö málfarsatriði. Í 12. gr. segir að aðgangur að sjúkraskrám sé óheimill nema „til þessa" standi lagaheimild. Betur færi á því ef í stað „til þessa" segði „til hans". Auk þess segir í bæði 18. gr. og 1. mgr. 19. gr. „sambærilegar trúnaðar- og þagnarskyldu". Þarna ætti að standa „sambærilega trúnaðar- og þagnarskyldu".

Að svo stöddu gerir Persónuvernd ekki frekari athugasemdir við frumvarpið en áskilur sér rétt til að koma viðbótarathugasemdum á framfæri síðar.

Í Persónuvernd 18. ágúst 2008

Páll Hreinsson
stjórnarformaður

Ólafur Garðarsson

Magnús Hafliðason

Vilhelmína Haraldsdóttir

Hjálagt:
Afrit af ákvörðun Persónuverndar frá 19. febrúar 2007 í máli nr. 2005/384

AFRIT

Persónuvernd
Data Protection Authority

Rauðarárstíg 10 105 Reykjavík Iceland
tel.: 354 510 9600 fax: 354 510 9606
e-mail: postur@personuvernd.is
web page: personuvernd.is

Reykjavík, 19. febrúar 2007
Tilvísun: 2005070384 ÞS/--

Ákvörðun

~~Hinn 19. febrúar 2007 tók stjórn Persónuverndar svohljóðandi ákvörðun í máli nr. 2005/384,~~ varðandi öryggi rafrænna sjúkraskráa innan Landspítala – Háskólasjúkrahúss (LSH) og aðgang að þeim.

I.
Málavextir og bréfaskipti

1.

Í framhaldi af fyrri samskiptum Persónuverndar og LSH bárust Persónuvernd, hinn 1. mars 2005, upplýsingar LSH, dags. 24. febrúar 2005, um aðgangsheimildir starfsmanna sjúkrahússins að rafrænum sjúkraskrám. Hjálögð var skrá yfir handhafa aðgangsheimilda. Kom fram að hún yrði lögð til grundvallar frá 3. mars 2005 og að læknar og hjúkrunardeildarstjórar myndu hafa aðgang að öllum sjúkraskrám allra klínískra skipulagskjarna sjúkrahússins. Sama ætti við um heilbrigðisstarfsmenn í skilgreindum teymum sem sinna sjúklingum víða á sjúkrahúsinu. Upplýsingar, sem talið væri að þyrftu sértæka vernd umfram aðrar sjúkraskráruppl ýsingar, yrðu þó varðveittar í sérstökum „hólfum" sem framangreindur aðgangur yrði ekki veittur að. Þetta ætti við um upplýsingar á geðsviði, sem og m.a. upplýsingar um viðkvæm, félagsleg atriði; tilurð sjúkdómsástands, s.s. ofbeldi; og frásagnir þriðja aðila.

Með bréfi, dags. 7. júlí 2005, óskaði Persónuvernd skýringa. Var spurt hvaða lagaheimildir LSH teldi standa til þess að haga aðganginum með framangreindum hætti. Þá var spurt um fyrirkomulag öryggismála. LSH svaraði með bréfi, dags. 24. ágúst 2005. Þar segir m.a.:

> „Í 1. gr. reglugerðar um sjúkraskrár og skýrslugerð varðandi heilbrigðismál (nr. 227/1991) segir [...]: „Sjúkraskrá [...] er safn sjúkragagna sem unnin eru eða fengin annars staðar frá vegna meðferðar einstaklinga hjá lækni eða heilbrigðisstofnun."
>
> Í 10. gr. reglugerðarinnar segir:
> „Við útskrift sjúklings frá heilbrigðisstofnun skal flytja öll rituð sjúkragögn saman í eina sjúkraskrá og

varðveita þau þannig í skjalasafni stofnunarinnar."

Af ákvæðum þessum leiðir að sjúkragögn eru varðveitt saman sem ein heild og læknir, er hefur aðgang að sjúkraskrá sjúklings, hefur aðgang að öllum upplýsingum í sjúkraskránni eins og hún er varðveitt á spítalanum.

Á Landspítala – háskólasjúkrahúsi er litið svo á að við meðferð sjúklinga skuli læknir afla sem fyllstra upplýsinga um öll þau atriði er skipt geta máli við meðferð viðkomandi sjúklings. Á það jafnt við um upplýsingar sem orðið hafa til á deild eða starfsstöð viðkomandi læknis og aðrar upplýsingar er orðið hafa til innan spítalans og varða heilsufar sjúklingsins. Aðgangur lækna að heildstæðum sjúkraskrárupplýsingum er því nauðsynlegur þegar sjúklingar koma til meðferðar. Lítur LSH svo á að slíkur aðgangur sé íþyngjandi skylda sem lögð er á herðar læknum spítalans."

Um öryggisráðstafanir segir m.a.:

„Í reglum LSH um aðgangsheimildir starfsmanna að heilsufarsupplýsingum, sem varðveittar eru á rafrænu formi á Landspítala – háskólasjúkrahúsi kemur fram að aðgangi að upplýsingum er stýrt með notkun persónutengds aðgangsorðs sem starfsmanni er úthlutað og hann ber persónulega ábyrgð á. Slíkt persónutengt aðgangsorð er einungis veitt í samræmi við fyrirmæli viðkomandi yfirlæknis, eða með ákvörðun framkvæmdastjóra lækninga. Með reglum sem settar eru af framkvæmdastjórn er ákveðið hverjir eigi að hafa aðgang að sjúkraskrárkerfinu og hvernig aðgangi að einstökum sjúkraskrám skuli verða háttað."

Þá segir að fram eigi að fara aðgerðaskráning þannig að skráð verði hverjir skoði sjúkraskrár og færi í þær upplýsingar. Með bréfi, dags. 9. september 2005, þakkaði Persónuvernd fram komin svör en bað um frekari skýringar. Í bréfi hennar segir m.a.:

„Persónuvernd þakkar þær skýringar sem borist hafa [...]. Hins vegar er jafnframt farið fram á frekari skýringar á þeim sjónarmiðum sem liggja að baki ákvörðun LSH um hinn víðtæka aðgang lækna að sjúkraskrám, þ.e. hvers vegna hann hafi verið talinn nauðsynlegur. Það sem Persónuvernd telur að koma verði fram í því sambandi er hvort tekið hafi verið tillit til þess hvernig starfssvið og einstök verkefni lækna eru mismunandi. Það birtist m.a. í því að læknar, sem fást við bráðatilvik, geta fengið sjúklinga til meðferðar fyrirvaralaust en að aðrir læknar fá sjúklinga iðulega til meðhöndlunar eftir fyrirfram ákveðinni röð. Einnig birtist það í hinni miklu sérhæfingu lækna, sem og því hversu misjöfn sú áhætta er sem fylgir einstökum verkefnum, t.d. meiri háttar skurðaðgerðum annars vegar og ýmsum minni háttar læknisverkum hins vegar."

LSH svaraði með bréfi, dags. 29. september 2005. Þar segir:

„Að baki ákvörðun LSH um hinn víðtæka aðgang lækna að sjúkraskrám liggja öryggissjónarmið, þ.e. sú staðreynd að sjúkraskrár eru öryggistæki í starfsemi spítalans. Lækni, sem fær sjúkling til meðferðar, þarf að vera ljóst, að svo miklu leyti sem mögulegt er, hvaða heilsufarsvandi hrjáir viðkomandi og það er í þágu öryggis sjúklingsins sem sjúkraskráin er gerð. Gildir þá einu hvort um bráðatilvik er að ræða eða hvort sjúklingur er tekinn til meðhöndlunar eftir fyrirfram ákveðinni röð. Þannig getur sjúkdómsþróun yfir lengri tíma haft mikla þýðingu við að greina vanda sjúklingsins og þarf þá m.a. að treysta á þær læknisskoðanir sem áður hafa verið framkvæmdar og sjúklingur getur ekki veitt fullnægjandi upplýsingar um, eðli málsins samkvæmt. Mörg önnur atriði er hægt að benda á í þessu sambandi. Jafnframt er rétt að benda á að langflestir, ef ekki allir, læknar sem sjá sjúklinga eftir fyrirfram ákveðinni röð þurfa jafnframt að sinna bráðavandamálum sem upp koma. Getur þar verið um að ræða bæði störf á móttöku og einnig störf á legudeildum spítalans, bæði innan og utan hefðbundins vinnutíma.

Sérhæfing lækna er vissulega misjöfn en eðli starfa þeirra er þó hið sama í öllum tilvikum, þ.e. að taka til meðferðar sjúklinga sem koma til þeirra og fela þeim þannig vissa ábyrgð á heilsufari sínu og lífi. Þar gildir einu hvort sjúklingar eru meðhöndlaðir með skurðaðgerðum eða með lyfjum sem oft á

tíðum eru mjög kröftug og geta leitt til dauða ef þau eru notuð á rangan hátt. Getur þar bæði verið um að ræða ranga skömmtun en jafnframt möguleika á milliverkunum lyfja, sem geta verið hættulegar þótt viðkomandi lyf séu skaðlítil hvort fyrir sig, í hefðbundnum skömmtum.

Enn sem komið er hafa fáir sérfræðingar er starfa á rannsóknarstofu LSH í meinafræði haft aðgang að SÖGU-kerfinu. Spítalinn áformar hins vegar að veita einnig þessum læknum aðgang, þar sem þeir geta þurft að hafa aðgang að upplýsingum um heilsufar sjúklinga á víðum grunni, t.d. þegar þeir skoða vefjasýni og setja sjúkdómsgreiningar sem meðferð byggist síðan á.

Landspítali – háskólasjúkrahús telur nauðsynlegt að öllum læknum spítalans sé mögulegt að lesa sjúkraskrár sjúklinga í þeim tilvikum er þeir koma að meðferð þeirra eða rannsóknum að einhverju leyti. Það er ítrekað að læknar spítalans hafa undirgengist þagnareið og að þeim er ljós ábyrgð sín að því er varðar trúnað við sjúklinga. Þeim er einnig kunnugt um hvernig heimilt er að nota sjúkragögn í störfum sínum á spítalanum og eru sjálfir hæfastir til að ákveða hvernig rétt er að nota gögnin hverju sinni. Jafnframt er ítrekað það eftirlit af hendi spítalans sem fram fer með notkun sjúkragagna. Komi í ljós að læknar fari út fyrir þær heimildir er þeir hafa til að nota sjúkragögn, mun spítalinn grípa til viðeigandi ráðstafana, svo sem fram kemur í reglum spítalans og Persónuvernd hafa verið kynntar."

Að fengnu þessu bréfi óskaði Persónuvernd þess, með bréfi dags. 11. október 2005, að haldinn yrði fundur með stjórnendum sjúkrahússins þar sem farið yrði yfir málið. Var þess einkum óskað að á fundinum yrði uppbygging hins rafræna sjúkraskrárkerfis útskýrð, öryggi rætt og hugmyndir um breytingar á kerfinu. Var þess og óskað að fulltrúum Persónuverndar yrði sýnt hvernig kerfið virkaði í framkvæmd.

Fundurinn var haldinn 16. nóvember 2005. Skömmu áður barst Persónuvernd bréf frá LSH um aðgang læknanema að rafrænum sjúkraskrám innan sjúkrahússins. Um það atriði verður hins vegar ekki fjallað að svo stöddu og efni þess bréfs LSH því ekki rakið hér.

2.

Á framangreindum fundi var farið yfir fyrirkomulag rafrænna sjúkraskráa. M.a. voru ræddar hugmyndir um skipan eftirlitsnefndar sem hafa myndi það hlutverk að skoða aðgerðaskráningar (log-skrár) til að ganga úr skugga um að starfsmenn færu ekki út fyrir aðgangsheimildir sínar. Þá var rætt um aðgerðaskráningu sem tryggði að sjá mætti hver hefði farið inn í hvaða gögn og hvað hann hefði gert. Þá var rædd sú hugmynd að hanna kerfið þannig að áður en farið væri inn í gögn yrði sá sem það gerði að tilgreina tilgang sinn, t.d. með því að haka í þar til gerðan reit.

Af hálfu LSH kom fram að ástæða þess að allir læknar, hjúkrunardeildarstjórar og ýmsir aðrir heilbrigðisstarfsmenn þyrftu að hafa aðgang að öllum sjúkraskrám allra klínískra skipulagskjarna sjúkrahússins væri sú að þeir þyrftu ýmist að veita ráðgjöf vegna læknismeðferðar, eða koma beint að henni, á öllu sjúkrahúsinu. Persónuvernd ræddi hvort einhverjum starfsmanna nægði ekki aðgangur að sjúkraskrám sjúklinga á tilgreindum deildum og nefndi m.a. þá starfsmenn sem almennt veita aðeins ráðgjöf út frá sérþekkingu sinni eða koma aðeins að meðferð á tiltekinni deild. Af hálfu LSH kom fram að það væri mjög erfitt því flestir læknar og hjúkrunardeildarstjórar færu um allt sjúkrahúsið.

Persónuvernd ræddi hvort loka mætti fyrir aðgang að sjúkraskrá þegar tiltekinn tími er liðinn frá því að sjúklingur útskrifast, þó þannig að aðgangur opnist sjálfkrafa innritist hann að nýju. LSH taldi meinbugi vera á þessu, enda lyti vinna heilbrigðisstarfsfólks mjög að sjúklingum með króníska sjúkdóma sem væru stöðugt til meðferðar – hvort sem þeir væru inni á sjúkrahúsinu eða ekki. Þá yrði að vera unnt að skoða sjúkraskrá þegar sjúklingar hefðu samband símleiðis. Var nefnt að stundum yrði að lesa upp úr sjúkraskrá fyrir starfsfólk á öðrum heilbrigðisstofnunum þegar sjúklingur væri til meðferðar þar.

Af hálfu LSH var tilkynnt að stefnt væri að því að fá, eigi síðar en um vorið 2006, vottun bresku staðlastofnunarinnar á að farið væri eftir öryggisstaðlinum ISO-17799. Af hálfu Persónuverndar var því þá lýst yfir að vinna stofnunarinnar varðandi fyrirkomulag og öryggi rafrænna sjúkraskráa á LSH myndi liggja niðri um sinn, eða a.m.k. til 1. maí 2006. Með bréfi Persónuverndar, dags. 10. mars 2006, var spurt hvernig innleiðingu öryggisstaðalsins ISO 27001 miðaði. LSH svaraði með bréfi, dags. 27. s.m., þar sem fram kom að vottunin myndi fást síðar en áætlað hafði verið. Hún myndi ekki fást þá um vorið heldur í nóvember 2006. Með bréfi, dags. 27. október s.á., óskaði Persónuvernd upplýsinga um hvað vinnunni liði. Svarað var með bréfi, dags. 21. nóvember 2006. Þar kom fram að úttekt bresku staðlastofnunarinnar vegna vottunarinnar myndi fara fram 4.–8. desember s.á. Í framhaldi af því sendi Persónuvernd LSH bréf, dags. 14. desember 2006, og óskaði þess að henni yrðu sendar niðurstöður vottunarinnar þegar þær lægju fyrir. Var þess sérstaklega óskað að upplýst yrði hvort vottunin hefði tekið til aðgangs að rafrænum sjúkraskrám. Til fróðleiks greindi Persónuvernd frá niðurstöðu úttektar sænsku persónuverndarstofnunarinnar, Datainspektionen, á sjúkraskrárkerfi sjúkrahússins í Karlstad, dags. 12. desember 2006.

Persónuvernd barst hinn 17. janúar 2007 tölvubréf frá LSH. Þar segir m.a.:

> „[...]Á Landspítala – háskólasjúkrahúsi (LSH) er notkun heilbrigðisstarfsmanns á heilsufarsupplýsingum í rafrænni sjúkraskrá skráð hvert sinn þegar skráin er opnuð. Þannig er hægt er að rekja hverjir hafa opnað hverja sjúkraskrá.
>
> Til að hafa eftirlit með notkun rafrænnar sjúkraskrár hefur verið sett á stofn eftirlitsnefnd er í eiga sæti 2 læknar og 1 hjúkrunarfræðingur. Nefndin er skipuð af framkvæmdastjóra lækninga á LSH og starfar í umboði hans. Formaður nefndarinnar er Stefán Yngvason læknir, sviðsstjóri lækninga á endurhæfingarsviði. Hefur nefndin sett sér starfsreglur og í þeim kemur fram að hlutverk nefndarinnar er m.a. eftirfarandi:
>
> Nefndin athugar uppflettiskýrslur sem unnar eru með rafrænum hætti í rafrænni sjúkraskrá. Sjúkraskrárnar eru tengdar kennitölu sjúklings og eru þær valdar af handahófi. Auk þess getur nefndin valið að skoða sjúkraskrár tiltekinna sjúklinga eða umgengi einstakra starfsmanna um sjúkraskrár. Komi fram vísbendingar um misnotkun skal það samstundis tilkynnt framkvæmdastjóra lækninga sem ber ábyrgð á eftirliti með meðferð og vörslu heilsufarsupplýsinga á LSH. Þar kemur einnig fram að brot á reglum um notkun rafrænnar sjúkraskrár og misnotkun trúnaðarupplýsinga um sjúklinga á LSH geta varðað áminningu eða brottrekstri úr starfi auk kæru ef um lögbrot er að ræða.
>
> Innan LSH er unnið að frekari þróun aðgangsstýringar og útfærslu eftirlits með notkun rafrænna sjúkraskráa."

Í bréfinu er og fjallað um aðgang læknanema að sjúkraskrám, en þar sem þessi ákvörðun tekur ekki til hans verður sá hluti bréfsins ekki reifaður hér.

3.

Á fundi stjórnar Persónuverndar hinn 22. janúar 2007 var mál þetta rætt. Þóttu ekki vera efni til að bíða lengur með að taka afstöðu til þeirra öryggisráðstafana sem viðhafðar eru á LSH varðandi aðgang að rafrænum sjúkraskrám. Var LSH, með bréfi dags. 31. janúar 2007, gert kunnugt um þetta og sjúkrahúsinu gefinn kostur á að koma að athugasemdum til viðbótar þeim sem það hafði þegar komið á framfæri – teldi það ástæðu til. Svarað var með tölvubréfi hinn 6. febrúar 2007, en með því fylgdi m.a. skjal frá bresku staðlastofnuninni, dags. 8. desember 2006, varðandi það hvort farið sé að öryggisstaðlinum ISO 27001 innan upplýsingatæknisviðs LSH. Eru þar gerðar ýmsar athugasemdir við öryggiskerfi persónuupplýsinga í ljósi ákvæða staðalsins.

Má þar nefna að talin er þörf á að tryggja betur að upplýsingatæknisviði berist skjótt ábendingar

þegar starfsmaður hefur störf á nýrri deild eða lætur af störfum (bls. 5 í skjalinu). Þá segir að hvorki liggi fyrir að fram fari reglubundin skoðun á því að við tilfærslu starfsmanna milli deilda sé aðgangsheimildum viðkomandi starfsmanns breytt (bls. 6) né hvernig staðið sé að veitingu kerfisstjóraaðgangs (bls. 7). Einnig segir að þegar starfsmönnum séu afhentir geisladiskar með tölfræðiupplýsingum, þar sem einnig sé að finna viðkvæmar persónuupplýsingar um sjúklinga, sé þess ekki gætt að dulkóða persónuupplýsingarnar (bls. 10). Auk þess er talin þörf á að bæta verklag við úthlutun nýrra aðgangsorða, m.a. til að tryggja að sá sem biður um aðgangsorð sé örugglega sá sem hann segist vera (bls. 11). Þá þurfi að koma á því fyrirkomulagi að þegar starfsmaður fer fyrst inn í tölvukerfi LSH, eftir að hafa fengið úthlutað aðgangsorði, þurfi hann að breyta aðgangsorði sínu (bls. 14).

Hinn 15. febrúar 2007 sendi Persónuvernd LSH tölvubréf með ósk um nánari skilgreiningu á því hvað það ætti við með „skilgreindum teymum". LSH svarði með tölvubréfi sama dag. Þar kemur fram að um er að ræða fjögur teymi, þ.e. líknarteymi, sýkingavarnateymi, útskriftar- og öldrunarteymi og teymi um sérhæfða heimaþjónustu fyrir veika aldraða. Í fyrstnefnda teyminu eru átta einstaklingar, því sem næst er nefnt eru einnig átta, í því sem nefnt er þar á eftir eru þeir 11 og í því síðastnefnda eru þeir fjórir. Segir að að mönnun teyma breytist með tímanum, en þó megi gera ráð fyrir að menntun og starfsheiti meðlima þeirra verði þau sömu. Þá sé líklegt að fleiri teymi verði sett á stofn, en fjöldi þeirra verði þó fyrirsjáanlega mjög takmarkaður.

II.
Niðurstaða Persónuverndar

Áður en unnt er að taka afstöðu til öryggis vinnslu persónuupplýsinga þarf að ákvarða hvort hún sé lögmæt.

Að því er varðar rafrænar sjúkraskrár verður ekki framhjá því litið að nokkuð skortir á skýrleika núgildandi laga og reglugerðarákvæða, enda bera þau þess merki að hafa að mestu leyti verið sett fyrir tilkomu slíkra skráa.

Með tilkomu rafrænna sjúkraskráa hafa forsendur fyrir aðgangi að þeim breyst. Notkun þeirra er orðin verulega útbreidd og samhliða hefur aðgangur að þeim orðið auðveldari og algengari. Í því ljósi telur Persónuvernd, þrátt fyrir skort á skýrum lagareglum, að ekki verði lengur undan því skorist að taka afstöðu til lágmarksöryggis varðandi aðgang að rafrænum sjúkraskrám. Áður verður þó, í samræmi við framangreint, að skoða lögmæti vinnslunnar.

1.

Að svo miklu leyti sem skráning og meðferð heilbrigðisupplýsinga byggist ekki á samþykki sjúklings er almennt talið að hún verði að byggjast á reglum sem settar hafa verið í lög, enda þótt heimilt sé að færa fyrirmæli þeirra nánar út í reglugerð. Byggir þetta á 1. mgr. 71. gr. stjórnarskrárinnar sem veitir sérhverjum manni friðhelgi um einkalíf sitt, en til að tryggja þá friðhelgi verður löggjafinn m.a. að gæta að því að lög leiði ekki af sér raunhæfa hættu á að viðkvæmar upplýsingar um einkahagi manns komist í hendur annarra sem eiga ekki réttmætt tilkall til aðgangs að þeim. Í réttinum til að njóta friðhelgi um einkalíf sitt felst m.a. réttur til að njóta verndar gegn óleyfilegum aðgangi að viðkvæmum persónuupplýsingum. Sett hafa verið í lög ákvæði um heimildir aðgangs þeirra heilbrigðisstarfsmanna að heilbrigðisupplýsingum *sem hans þurfa nauðsynlega í þágu læknismeðferðar,* en aðrir heilbrigðisstarfsmenn hafa ekki sambærilegar heimildir.

Mat á lögmæti fyrirkomulags aðgangs starfsmanna á LSH að rafrænum sjúkraskrám ræðst af framangreindu og túlkun á ákvæðum laga nr. 77/2000, sbr. og eftir atvikum á ákvæðum í sérlögum.

2.

Lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga

Gildissvið laga nr. 77/2000 og verkefnasvið Persónuverndar nær til vinnslu persónuupplýsinga, sbr. 1. mgr. 3. gr. og 1. og 2. mgr. 37. gr. laganna. *Persónuupplýsingar* eru sérhverjar persónugreindar eða persónugreinanlegar upplýsingar, þ.e. upplýsingar sem beint eða óbeint má rekja til tiltekins einstaklings, látins eða lifandi, sbr. 1. tölul. 2. gr. *Vinnsla* er sérhver aðgerð eða röð aðgerða þar sem unnið er með persónuupplýsingar, hvort heldur sem vinnslan er handvirk eða rafræn, sbr. 2. tölul. 2. gr.

Svo að vinnsla persónuupplýsinga sé heimil þarf ávallt að vera fullnægt einhverju skilyrðanna í 8. gr. laga nr. 77/2000. Svo að vinnsla *viðkvæmra* persónuupplýsinga sé heimil þarf að auki að vera fullnægt einhverju skilyrðanna í 1. mgr. 9. gr. sömu laga. Upplýsingar í sjúkraskrám eru viðkvæmar, sbr. c-lið 8. tölul. 2. gr. laganna. Þarf færsla þeirra og aðgangur að þeim því bæði að eiga sér stoð í einhverju af ákvæðum 1. mgr. 8. gr. og einhverju af ákvæðum 1. mgr. 9. gr. laganna.

Ljóst er að flestir töluliðir 1. mgr. 8. gr. geta komið til greina, allt eftir aðstæðum hverju sinni, þ. á m. 1. tölul. um samþykki viðkomandi sjúklings. Af ákvæðum 1. mgr. 9. gr. koma 1., 2. og 8. tölul. helst til greina. Í 1. tölul. er mælt fyrir um að vinnsla sé heimil þegar samþykki er fyrir hendi, í 2. tölul. um að vinnsla sé heimil sé sérstaka heimild fyrir henni að finna í öðrum lögum og í 8. tölul. um að vinnsla sé heimil í þeim tilvikum þegar hún er nauðsynleg vegna læknismeðferðar eða vegna venjubundinnar stjórnsýslu á sviði heilbrigðisþjónustu, enda sé hún framkvæmd af starfsmanni þjónustunnar sem bundinn er þagnarskyldu.

Við mat á lögmæti verður einnig að líta til skilyrða 1. mgr. 7. gr. laga nr. 77/2000 um gæði gagna og vinnslu. Þessi skilyrði eru m.a. að persónuupplýsingar skulu unnar með sanngjörnum, málefnalegum og lögmætum hætti og að öll meðferð þeirra skal samrýmast vönduðum vinnsluháttum persónuupplýsinga (1. tölul.); að þær skulu fengnar í yfirlýstum, skýrum, málefnalegum tilgangi og ekki unnar frekar í öðrum og ósamrýmanlegum tilgangi (2. tölul.); og að þær skulu vera nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilgang vinnslunnar (3. tölul.). Til samans fela þessi ákvæði í sér grundvallarreglu um meðalhóf sem m.a. birtist í því að aðgangur að persónuupplýsingum skal ekki að vera víðtækari en nauðsyn krefur.

3.

Sérlagaákvæði um sjúkraskrár

Ekki er skilgreint í lögum nr. 74/1997 hvað átt sé við með sjúkraskrá, en slíka skilgreiningu er að finna í 1. gr. reglugerðar nr. 227/1991 um sjúkraskrár og skýrslugerð varðandi heilbrigðismál, sbr. 6. mgr. 14. gr. laganna. Hún hljóðar svo:

> „Sjúkraskrá [...] er safn sjúkragagna sem unnin eru eða fengin annars staðar frá vegna meðferðar einstaklinga hjá lækni eða í heilbrigðisstofnun.
>
> Sjúkragögn í sjúkraskrá geta verið lýsing eða túlkun í rituðu máli, myndir, þ.m.t. röntgenmyndir, línurit eða upptaka sem numin hefur verið með hjálp tæknibúnaðar. Gögnin innihalda upplýsingar um heilsufar og aðra einkahagi viðkomandi einstaklinga og tímasettar upplýsingar um það sem gerist eða gert er meðan einstaklingurinn er í meðferð hjá lækni eða í heilbrigðisstofnun."

Um réttindi sjúklinga er fjallað í lögum nr. 74/1997. Í 1. mgr. 14. gr. laganna segir að sjúkraskrá skuli varðveitt á heilbrigðisstofnun þar sem hún er færð eða hjá lækni eða öðrum heilbrigðisstarfsmanni sem hana færir á eigin starfsstofu. Einnig kemur m.a. fram, í 1. mgr. 15. gr.

laganna, að þess skal gætt við aðgang að sjúkraskrám að þær hafa að geyma viðkvæmar persónuupplýsingar og að upplýsingar í þeim eru trúnaðarmál. Í 2. mgr. 15. gr. mælt fyrir um að sjúkraskrá skuli geymdar á tryggum stað og að þess skuli gætt *að einungis þeir starfsmenn, sem nauðsynlega þurfa, hafi aðgang að þeim.* Er þetta ákvæði í samræmi við framangreinda meðalhófsreglu 7. gr. laga nr. 77/2000.

3.

Sjónarmið LSH

LSH hefur vísað til þess að sjúkraskrá einstaklings sé heildarsafn þeirra sjúkragagna sem til verða um hann innan heilbrigðisstofnunar, sbr. 10. gr. reglugerðar nr. 227/1991. Því sé eðlilegt að veita aðgang að rafrænni skrá í heild sinni en ekki aðeins að tilteknum hlutum hennar.

Þá hefur LSH rökstutt tilhögun aðgangs umræddra starfsmanna að rafrænum sjúkraskrám með því að enda þótt viðkomandi vinni ekki á þeirri deild þar sem sjúklingur nýtur læknismeðferðar, og komi þar beint að þeirri meðferð, sinni þeir störfum víða innan sjúkrahússins og hvorki sé með góðu móti unnt að afmarka aðgangsþörf þeirra við tiltekna sjúklinga né við upplýsingar sem varðveittar eru á tilteknum deildum. Hefur sjúkrahúsið útskýrt að heilbrigðisstarfsfólk af ýmsum deildum vinni saman og að sérþekking starfmanna á tilteknum deildum nýtist og sé *nauðsynleg* við meðferð sjúklinga á öðrum deildum. Þetta eigi ekki aðeins við um lækna og hjúkrunardeildarstjóra heldur og heilbrigðisstarfsmenn sem vinna undir þeirra handleiðslu í tengslum við að veita læknismeðferð.

5.

Ákvörðun Persónuverndar

um lögmæti, meðalhóf og öryggi

Á Landspítala – Háskólasjúkrahúsi hafa læknar og hjúkrunardeildarstjórar aðgang að öllum sjúkraskrám allra klínískra skipulagskjarna sjúkrahússins. Sama á við um heilbrigðisstarfsmenn í líknarteymi, sýkingavarnateymi, útskriftar- og öldrunarteymi og teymi um sérhæfða heimaþjónustu fyrir veika aldraða. Má rökstyðja heimildir til þessa með vísun til 1. mgr. 8. gr. og 1. og 8. tl. 1. mgr. 9. gr. laga nr. 77/2000.

Auk þess að uppfylla framangreind skilyrði verður vinnsla að fullnægja skilyrðum 7. gr. laga 77/2000, sbr. og 2. mgr. 15. gr. laga nr. 74/1997. Í ljósi framangreindra röksemda LSH, um nauðsyn aðgangs vegna læknismeðferðar, mun Persónuvernd ekki að svo stöddu endurskoða ákvörðun sjúkrahússins um aðgang framangreindra starfsmanna að rafrænum sjúkraskrám. Dregur hún því ekki í efa að lög standi til aðgangs þeirra að sjúkraskrám, enda séu uppfyllt ákvæði 11. gr. laga nr. 77/2000 um upplýsingaöryggi.

Í „upplýsingaöryggi" felast þrír grundvallarþættir: (a) Að persónuupplýsingum sé leynt gagnvart óviðkomandi, (b) að þær séu áreiðanlegar og (c) að þær séu aðgengilegar þeim sem nauðsynlega þurfa á þeim að halda. Allir þessir þættir eru mikilvægir við vernd sjúkraskrárupplýsinga, en almennt er þó talið að við notkun þeirra í heilbrigðisþjónustu vegi áreiðanleiki upplýsinga og nauðsynlegt aðgengi heilbrigðisstarfsmanna að þeim þyngst, enda er hvoru tveggja mikilvægt til að tryggja góða heilbrigðisþjónustu. Með því er þó ekki gert lítið úr mikilvægi leyndar gagnvart óviðkomandi.

Samkvæmt ákvæði 11. gr. laga nr. 77/2000 skal *ábyrgðaraðili* að vinnslu persónuupplýsinga, þ.e. sá sem ákveður hvers vegna og hvernig vinna skal með slíkar upplýsingar, sbr. 4. tölul. 2. gr. laga nr. 77/2000 – í þessu tilviki LSH – gera viðeigandi tæknilegar og skipulagslegar öryggisráðstafanir til að vernda upplýsingarnar gegn ólöglegri eyðileggingu, gegn því að þær glatist eða breytist fyrir slysni og gegn óleyfilegum aðgangi. Varðandi öryggi og aðgang að rafrænum sjúkraskrám má

með mikilli einföldun segja að velja verði á milli tveggja höfuðsjónarmiða: (a) að leggja megináherslu á setningu strangra reglna um *aðgangsstýringar,* er endurspegli raunverulega þörf fyrir aðgang, eða (b) að leggja megináherslu á virkt *eftirfarandi eftirlit* með notkun aðgangsheimilda. Því minni áhersla, sem lögð er á strangar reglur um aðgangsstýringar, þeim mun meiri áherslu þarf að leggja á eftirfarandi eftirlit. Af hálfu LSH hefur því verið lýst yfir að miklir meinbugir séu á setningu strangra reglna um aðgangsstýringar því flestir læknar og hjúkrunardeildarstjórar fari um allt sjúkrahúsið. Sama eigi við um heilbrigðisstarfsmenn í líknarteymi, sýkingavarnateymi, útskriftar- og öldrunarteymi og teymi um sérhæfða heimaþjónustu fyrir veika aldraða.

Auk öryggisráðstafana í formi aðgangsstýringa og eftirfarandi eftirlits þarf að gæta annarra mikilvægra öryggisráðstafana. Má nefna að þar getur dulkóðun komið til greina og geta aðgangsorð þá virkað sem afkóðunarlyklar þannig að þegar starfsmenn slá þau inn afkóðist þær upplýsingar sem hver og einn nauðsynlega þarf í þágu starfa sinna. Á þetta er minnt í niðurstöðu starfshóps samkvæmt 29. gr. tilskipunar nr. 95/46/EB (sem liggur lögum nr. 77/2000 til grundvallar) um vinnslu persónuupplýsinga í rafrænum sjúkraskrám (sjá bls. 20 í skjalinu). Skjalið, sem útgefið er 15. febrúar 2007, hefur leiðbeinandi gildi um verndun rafrænna sjúkraskráa innan allra aðildarríkja EES-samningsins.

ÁKVÖRÐUN

Í samræmi við framangreint hefur Persónuvernd ákveðið, sbr. 40. gr. laga nr. 77/2000, að Landspítali – Háskólasjúkrahús skuli, fyrir 1. maí 2007, hafa komið á eftirfarandi öryggisráðstöfunum:

1. Allur aðgangur að rafrænum sjúkraskrám skal vera háður því að viðkomandi starfsmaður þurfi hann nauðsynlega starfs síns vegna og að hann noti sérstakt *persónubundið aðgangsorð* í hvert sinn sem hann opnar sjúkraskrá. Skal hann ávallt tilgreina tilganginn, s.s. með því að haka við tiltekinn reit.

2. Sérstök nefnd á vegum stjórnar LSH skal hafa með höndum úthlutun aðgangsorða. Skal líftími aðgangsorða vera að hámarki fjórir mánuðir.

3. Færa skal í *aðgerðaskrár (log-skrár)* upplýsingar um alla skoðun sjúkraskráa og færslu upplýsinga í þær.

4. Sérstök eftirlitsnefnd skal fylgjast með aðgerðaskráningu (log-skrám) og starfa eftir verklagsreglum sem stjórn LSH setur. Með þeim skal tryggt að nefndin hafi kerfisbundið og virkt eftirlit með öllum handhöfum aðgangsheimilda/ aðgangsorða. Skal hún skila skýrslu um störf sín til stjórnar LSH eigi sjaldnar en tvisvar á ári.

5. Gera skal greinarmun á upplýsingum í sjúkraskrám eftir eðli þeirra og hafa upplýsingar, sem þurfa sértæka vernd, í sérstaklega *vörðum „hólfum"*. Þetta á við um upplýsingar á geðsviði, sem og m.a. upplýsingar um viðkvæm, félagsleg atriði; tilurð sjúkdómsástands, s.s. ofbeldi; og frásagnir þriðja aðila. Þær skulu aðeins aðgengilegar starfsfólki á þeirri deild þar sem upplýsingar í umrædd hólf eru skráð.

6. Við skoðun persónuupplýsinga samkvæmt 5. tölul. skal tilgreina *ástæðu til viðbótar* því sem gera þarf samkvæmt 1. tölul. Hið sama gildir þegar skoðaðar eru sjúkraskrár manna sem ekki hafa verið til meðferðar á sjúkrahúsinu í sex mánuði eða lengur, sem og þegar starfsfólk á öðrum deildum en þeirri þar sem sjúklingur er til meðferðar þarf að skoða sjúkraskrá hans.

7. Í þeim tilvikum, sem tilgreind eru í 6. tölul., skal skoðun á persónuupplýsingum merkt

sérstaklega í aðgerðaskrám (log-skrám) til að auðvelda eftirlit þeirrar nefndar sem starfar samkvæmt 4. tölul. Skal hún, eigi sjaldnar en á þriggja mánaða fresti, gera sérstakar athuganir á skoðun þessara persónuupplýsinga og skila skýrslu um niðurstöður þeirra athugana til stjórnar LSH.

8. Fara skal yfir þær athugasemdir bresku staðlastofnunarinnar, sem raktar eru í lið 3 í I. kafla hér framar, og gera viðeigandi úrbætur í ljósi þeirra.

9. Gera skal reglulega *innri úttekt* á fyrirkomulagi öryggismála, þ. á m. hvort unnið sé í samræmi við framangreinda skilmála. Árlega skal skila skýrslum um framkvæmd slíkra úttekta til stjórnar LSH.

Ákvörðun þessi gildir til 19. febrúar 2010.

Reykjavík, 19. febrúar 2007

Páll Hreinsson
stjórnarformaður

Haraldur Briem

Valur Árnason

Ólafur Garðarsson