Ábyrgð lækna og vistun rafrænna trúnaðarupplýsinga

Guðjón Viðar Valdimarsson

Fáar starfstéttir eiga eins mikið undir trúnaði við sína umbjóðendur eins og læknar. Ljóst er að ef ekki er fullt traust milli sjúklings og læknis eða á milli lækna um samskipti með trúnaðarupplýsingar samkvæmt 5. mgr. 15. gr. læknalaga þá er vegið að starfsgrundvelli viðkomandi læknis.

Öryggi trúnaðarupplýsinga ætti því að vera forgangsmál hjá læknum en spurning er hvort svo sé í raun og veru. Nú eru nánast allar upplýsingar um sjúklinga og meðferð þeirra vistaðar rafrænt og það eykur mjög skilvirkni og hagkvæmni í meðferð þeirra. Það breytir hins vegar engu um lagaskyldu lækna gagnvart sjúklingum að gögn séu vistuð rafrænt og þó að framkvæmd þess öryggis sé falið tölvusérfræðingum yfirfærist ábyrgð lækna ekki með því. Það hljómar ekki vel að þurfa að útskýra fyrir sjúklingi að óheppilegar upplýsingar um hann séu komnar út um allt vegna þess að brotist hafi verið inn í tölvukerfið og þeim stolið.

Segja má að vandi lækna liggi í að lagaskyldan sé klárlega á þeirra herðum en vegna forms upplýsinganna sé framkvæmd þess öryggis í raun undir forsjá annarra. Spurningin er þá sú hvort þetta sé ásættanlegt ástand og þá hvort einhver ástæða sé til að breyta því eða hvort í raun sé einhver möguleiki á því.

Segjum sem svo að eftir lestur þessarar greinar taki hver læknir fyrir sig upp á því að vista trúnaðarupplýsingar á staðardrifi í ónettengdri tölvu á skrifstofu sinni. Ekki væri víst að öryggi upplýsinga batnaði mikið við það. Þar er þó vissulega verið að færa ábyrgð á þagnarskyldu og framkvæmd þeirrar ábyrgðar nær hvort öðru en samt er ekki víst að öryggi gagnanna aukist að sama skapi. Það er nefnilega ekki það að hættara sé við að brotist verði inn í gögn á netdrifum eða miðlægum kerfum, heldur fremur að þau eru vistuð á formi sem er aðgengilegt fyrir alla sem á annað borð komast yfir aðgang að þeim. Þetta er spurning um form gagna frekar en aðgang.

Heppilegast væri ef hægt væri að breyta formi gagna þannig að trúnaðarupplýsingar væru ólæsilegar öllum nema þeim sem hefðu lykil til að umbreyta þeim í læsilegt form. Þá væri vistun gagna ekki lengur aðalatriði heldur fremur að tryggja reglulegt afrit gagna og það er eitthvað sem viðkomandi læknir getur gengið úr skugga um án sérstaks tæknilegs bakgrunns.

Í dag er þetta hægt með því að breyta formi gagna í að vera vistuð á dulkóðuðu formi en séu gögn vistuð þannig skiptir ekki máli hver er með aðgang að þeim gögnum. Núverandi staðall hjá bandaríska varnarmálaráðuneytinu kallast AES (Advanced Encryption Standard) og gögn vistuð þannig nota allt að 256 bita dulkóðun og það er nánast ógerlegt að brjótast inn í þau og þar að auki er mögulegt að setja kerfið upp þannig að viðkomandi læknir sé með eiginlegan lykil að gögnum sínum sem handhafi dulmálslykils þeirra.

Öll dulkóðuð gögn byggja á dulmálslyklum til vistunar og endurheimtu og ef þessir lyklar eru vistaðir á tölvulyklum (USB), snjallkortum eða öðrum slíkum miðlum þá er viðkomandi læknir með fulla stjórn á öryggi viðkomandi gagna og ábyrgð þagnarskyldu og framkvæmd hennar fer betur saman.

Venjulega er aðgangur að þessum dulkóðuðu gögnum ekki einungis tryggður með að vera handhafi tölvulykils sem inniheldur réttu dulmálslyklana, heldur þarf viðkomandi að vita tiltekin aðgangsorð að auki.

Þetta form aðgangs er kallað tveggja þátta aðgangskerfi (two factor authentication) og er ekki bara notað við auðkenningu til að nálgast gögn heldur líka til auðkenningar inn á margvísleg tölvukerfi eins og vefpóst og sýndareinkanet (virtual private network, VPN)

Sú tækni sem notuð er við að dulkóða vistuð gögn er hins vegar ekki nauðsynlega sú tækni sem heppilegust er við sendingu trúnaðarupplýsinga til annarra lækna eða heilbrigðisstarfsmanna samkvæmt 5. mgr. 15. gr. læknalaga. Samskipti af þessu tagi eru oftar en ekki með tölvupósti og í sjálfu sér er ekkert að því ef réttum aðferðum er beitt til að vernda gögnin.

Þó má segja að ef um er að ræða sendingar á trúnaðarskjölum í tölvupósti þá sé um sama grundvallarvandamál að ræða og við vistun skjala. Eins og varðandi vistun skjala þá er það ekki nauðsynlega aðgangur að skjölunum heldur form þeirra en það sem er sérstakt við samskipti til dæmis í tölvupóst er að þá bætist við auðkenning og dreifing á dulmálslykli.

Sú tækni sem beitt er í dag varðandi þessa tegund samskipta heitir dreifilyklaaðferð (public key infrastructure). Þessi tækni gerir viðkomandi lækni kleift að senda trúnaðarskjöl í tölvupósti á dulkóðuðu formi og vera þess fullviss að þau sé verið að senda til rétts viðtakanda og einungis hann geti opnað gögnin. Einnig getur viðtakandi verið þess fullviss að sendandi sé sá sem hann segist vera.

Höfundur er framkvæmdastjóri Dulkóðun Islandia
www.dulkodun.is