

FINLANDS FÖRFATTNINGSSAMLING

Utgiven i Helsingfors den 31 mars 2014

250/2014

Lag

om ändring av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården

Utfärdad i Helsingfors den 28 mars 2014

I enlighet med riksdagens beslut

ändras i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007) 2 § 3 mom., 3 § 7 och 8 punkten, 5 § 2 mom., 14 § 1 mom., 14 a § 3 och 4 mom., 17—19 §, 20 § 4 och 5 mom. och 22 §,

av dem 2 § 3 mom., 20 § 4 och 5 mom. och 22 § sådana de lyder i lag 981/2010, 3 § 8 punkten sådan den lyder i lag 928/2011 samt 14 § 1 mom., 14 a § 3 och 4 mom. samt 17 och 19 § sådana de lyder i lag 1227/2010, samt

fogas till 3 §, sådan den lyder delvis ändrad i lagarna 1227/2010 och 928/2011, en ny 6 punkt i stället för den 6 punkt som upphävts genom lag 1227/2010, samt nya 9 och 10 punkter, till 16 §, sådan den lyder delvis ändrad i lagarna 981/2010 och 1227/2010, ett nytt 5 mom. i stället för det 5 mom. som upphävts genom lag 981/2010 samt till lagen nya 5 a—5 c kap. och nya 20 a—20 h § som följer:

2 §

Tillämpningsområde

Om inte något annat följer av denna eller någon annan lag tillämpas på behandlingen av klientuppgifter vad som bestäms i lagen om patientens ställning och rättigheter (785/1992), nedan *patientlagen*, lagen om klientens ställning och rättigheter inom socialvården (812/2000), nedan *klientlagen*, personuppgiftslagen (523/1999), lagen om offentlighet i myndigheternas verksamhet

(621/1999), lagen om elektronisk kommunikation i myndigheternas verksamhet (13/2003), lagen om stark autentisering och elektroniska signaturer (617/2009), lagen om befolkningsdatasystemet och Befolkningsregistercentralens certifikattjänster (661/2009) och arkivlagen (831/1994) eller i bestämmelser som utfärdats med stöd av dem. Vid behandlingen av klientuppgifter och ordnande av tjänster och funktioner enligt denna lag ska dessutom iakttas vad som föreskrivs i språklagen (423/2003) och med stöd av den. Om det informationssystem där hälso- och

sjukvårdens klient- och patientuppgifter behandlas är en sådan utrustning för hälso- och sjukvård som avses i lagen om produkter och utrustning för hälso- och sjukvård (629/2010) tillämpas på informationssystemet även den lagen och kraven i enlighet med den.

3 §

Definitioner

I denna lag avses med

6) *informationssystem* en programvara eller ett system för elektronisk behandling av klientuppgifter inom socialvården eller hälso- och sjukvården som används för lagring och uppdatering av klient- eller journalhandlingar och uppgifter i dem samt dataregister eller datalager bestående av insamlade uppgifter som förvaltas med hjälp av automatisk databehandling och som tillverkaren uttryckligen har planerat för behandlingen av klient- eller journalhandlingar inom socialvården eller hälso- och sjukvården och uppgifterna i dem; med informationssystem avses dessutom sådan förmedlingsservice varmed klientuppgifter inom socialvården eller hälso- och sjukvården förmedlas till de riksomfattande informationssystemtjänster enligt 14 § 1 mom. som Folkpensionsanstalten förvaltar,

7) *tillhandahållare av hälso- och sjukvårdstjänster* en verksamhetsenhet för hälso- och sjukvård enligt 2 § 4 punkten i patientlagen, en arbetsgivare enligt 7 § 2 punkten i lagen om företagshälsovård (1383/2001) samt en yrkesutbildad person inom hälso- och sjukvården som är självständig yrkesutövare,

8) *tillhandahållare av socialvårdstjänster* en myndighet som ordnar sådan socialvård som avses i 3 § 2 punkten i klientlagen, en offentlig producent av socialservice och en serviceproducent enligt lagen om privat socialservice (922/2011),

9) *bedömningsorgan för informationssäkerhet* sådana företag, sammanslutningar och myndigheter som Kommunikationsverket med stöd av lagen om bedömningsorgan för informationssäkerhet (1405/2011) har godkänt att utföra bedömningar av överensstämmelse med kraven i fråga om informationssystem, samt

10) *interoperabilitet* informationssystemens tekniska och innehållsliga förmåga att fungera tillsammans med övriga informationssystem när systemen utnyttjar samma information.

5 §

Uppföljning av användning och utlämnande

En tillhandahållare av tjänster ska för uppföljningen särskilt för varje klientregister samla in logguppgifter om all användning och om varje utlämnande av klientuppgifter i ett loggregister. I användningsloggregistret lagras uppgifter om använda klientuppgifter, den tillhandahållare av tjänster vars klientuppgifter används, vem som har använt klientuppgifterna, användningsändamålet och användningstidpunkten. I utlämningsloggregistret lagras uppgifter om utlämnade klientuppgifter, den tillhandahållare av tjänster vars klientuppgifter utlämnas, vem som lämnat ut klientuppgifterna, utlämningsändamålet, mottagaren och utlämningsstidpunkten. Folkpensionsanstalten ska samla in motsvarande information om utlämnande av uppgifter som lagrats i och visats via patientens informationshanteringstjänst som avses i 14 a §.

14 §

Riksomfattande informationssystemtjänster

För tillhandahållarna av hälso- och sjukvårdstjänster sköter Folkpensionsanstalten en arkiveringstjänst för förvaringen och användningen av journalhandlingar samt som en del av tjänsten, för utlämnandet av journalhandlingar, en katalogtjänst och patientens informationshanteringstjänst. I arkiveringstjänsten får det utöver journalhandlingarna lagras även andra handlingar som anknyter till ordnandet av hälso- och sjukvården och till informationshanteringen. Folkpensionsanstalten sköter dessutom inom ramen för de riksomfattande informationssystemtjänsterna förvaringen av utlämningsloggregistren som en del av arkiveringstjänsten, det medborgar-

gränssnitt som avses i 19 § och den tjänst genom vilken de riksomfattande informationssystemtjänsterna kan användas via internet och med mobila apparater med hjälp av telekommunikationsnät. Folkpensionsanstalten kan även ha hand om andra riksomfattande tjänster som anknyter till social- och hälsovårdens informationshantering enligt vad som särskilt föreskrivs om dem någon annanstans, samt sköta förvaringen av användningsloggregistren. Folkpensionsanstalten får vid behov meddela anvisningar om de tekniska konfigurationer och de definitioner för meddelandetrafiken som realiseringen av de ovannämnda riksomfattande informationssystemtjänsterna kräver.

14 a §

Patientens informationshanteringstjänst

Via patientens informationshanteringstjänst kan även sådana uppgifter som är viktiga med tanke på patientens hälso- och sjukvård eller anknyttande tjänster visas. Bestämmelser om vilka uppgifter som är sådana viktiga uppgifter som ska visas via informationshanteringstjänsten får utfärdas genom förordning av social- och hälsovårdsministeriet. Sådana uppgifter vars utlämnande patienten förbjudit med stöd av 10—12 § får dock inte visas via informationshanteringstjänsten.

Folkpensionsanstalten är registerförare för patientens informationshanteringstjänst. Folkpensionsanstalten ansvarar för tillgängligheten och integriteten i fråga om uppgifterna i informationshanteringstjänsten, datainnehållets oföränderlighet samt för förvaring och utplåning av uppgifterna. Den som lagrar uppgifter i patientens informationshanteringstjänst ansvarar för att uppgifterna är korrekta och för att felaktiga uppgifter som finns i tjänsten rättas. Vid rättelse av felaktiga uppgifter i informationshanteringstjänsten ska 29 § i personuppgiftslagen tillämpas. Om en felaktig uppgift är baserad på en anteckning som gjorts av en tillhandahållare av hälso- och sjukvårdstjänster ska yrkande om rättelse riktas till den tillhandahållare som gjort den felaktiga anteckningen.

16 §

Ansvar vid skötseln av informationssystemtjänsterna

Folkpensionsanstalten kan upprätta och lämna ut sammanställningar över sådan beskrivande information om uppgifterna i arkiveringstjänsten som kan ha betydelse för utvecklingen och uppföljningen av de riksomfattande informationssystemtjänsterna eller för rapporteringen. Dessutom kan Folkpensionsanstalten på de grunder som anges i 13 § 2—5 mom. i patientlagen lämna ut sådana uppgifter enligt 14 a § 2 mom. i denna lag om en patients viljeytringar som finns i patientens informationshanteringstjänst.

17 §

Information till patienten

Tillhandahållare av hälso- och sjukvårdstjänster som anslutit sig till de riksomfattande informationssystemtjänsterna ska informera patienten om de riksomfattande informationssystemtjänsterna, om deras allmänna verksamhetsprinciper och om patientens rättigheter i fråga om dem. Informationen ska lämnas före den första servicehändelsen eller i samband med den. Dessutom ska patienten informeras om vem som ordnar informationssystemtjänsterna, förutsättningarna för utlämnande av patientuppgifter, skyddet av informationen och om andra omständigheter i samband med behandlingen av uppgifter som är av betydelse för patienten.

Tillhandahållaren av hälso- och sjukvårdstjänster ska informera patienten personligen, skriftligt eller muntligt. Informationen får också ges med hjälp av en elektronisk tjänst som specificerar patienten. Om informationen ges på annat sätt än skriftligen ska patienten också kunna få den skriftligt. En anteckning om att information har getts ska göras i patientens informationshanteringstjänst som avses i 14 a §. Om patienten redan har fått informationen, får undantag göras från upplysningsplikten i enlighet med 24 § i personuppgiftslagen.

Vid behov får närmare bestämmelser om

förfarandet i fråga om sätten att informera och om informationens innehåll utfärdas genom förordning av social- och hälsovårdsministeriet.

18 §

Klientens rätt att få uppgifter

Bestämmelser om klientens rätt att kontrollera uppgifter i klientregistret och om tillgodeendet av denna rätt finns i 26—28 § i personuppgiftslagen.

För utredning eller utövande av sina rättigheter i anslutning till behandlingen av sina klientuppgifter har en klient rätt att på grundval av en skriftlig begäran utan dröjsmål av tillhandahållaren av socialvårdstjänster och hälso- och sjukvårdstjänster på grundval av loggregistret avgiftsfritt få veta vem som har använt eller till vem man har utlämnat uppgifter om honom eller henne samt grunden för användningen eller utlämnandet. Klienten har motsvarande rätt att av Folkpensionsanstalten få information om utlämnande av uppgifter som lagrats i och som visas via patientens informationshanteringstjänst som avses i 14 a §. Klienten har dock inte rätt att få logguppgifter, om den som lämnar ut logguppgifter vet att utlämnandet av logguppgifterna kan medföra allvarlig fara för klientens hälsa eller vård eller för någon annans rättigheter. Klienten har inte heller rätt att utan särskild orsak få logguppgifter som är äldre än två år. Klienten får inte för något annat ändamål använda eller vidareutlämna logguppgifter som han eller hon erhållit.

Om en klient för andra gången begär logguppgifter som gäller samma tidsperiod kan tillhandahållaren av tjänster eller Folkpensionsanstalten ta ut en skälig ersättning för lämnandet av dessa logguppgifter, som inte får överstiga de direkta kostnaderna för lämnandet av informationen. För tillträde till logguppgifter med hjälp av den elektroniska förbindelse som avses i 19 § får dock ingen separat avgift tas ut.

Om en klient anser att hans eller hennes klientuppgifter har använts eller lämnats ut utan tillräckliga grunder ska den tillhandahållare av tjänster som använt eller fått uppgifterna eller Folkpensionsanstalten på begäran

ge klienten en utredning om grunderna för användningen eller utlämnandet av uppgifterna.

19 §

Medborgargränssnitt

Patienten ges med hjälp av ett medborgargränssnitt följande uppgifter som gäller honom eller henne och som är lagrade i den riksomfattande arkiveringstjänsten:

1) uppgifter om samtycken och förbud samt utlämningslogguppgifter, med undantag för utlämnarens och mottagarens personuppgifter samt de utlämningslogguppgifter som patienten enligt 27 § 1 mom. 1—4 punkten i personuppgiftslagen inte har rätt att få,

2) uppgifter om organdonationsförbud, livstestamenten och patientens övriga viljeyttringar som gäller hälso- och sjukvården eller organdonation som införts i patientens informationshanteringstjänst,

3) uppgifter om tid och plats för servicehändelser, uppgifter som är viktiga med tanke på vården, uppgifter om läkemedelsordinationer och vårdföreskrifter, och

4) remisser, sammandrag av den vård som getts, slutgiltiga utlåtanden om vården samt läkarintyg och läkarutlåtanden.

Med hjälp av medborgargränssnittet kan patienten också ges uppgifter om tidsbeställningar samt laboratorieresultat, diagnostiska utbildningsresultat och andra motsvarande undersökningsresultat. Till medborgargränssnittet får, utöver de funktioner som nämns i 1 mom., dessutom anslutas andra funktioner som möjliggör informationsåtkomst för patienten och gör det möjligt att genomföra och följa upp uppgifter som i övrigt anknyter till vården och hälso- och sjukvården.

Oberoende av 1 och 2 mom. ska gränssnittet realiseras så att patienten inte har åtkomst till de uppgifter vilkas utlämnande en yrkesutbildad person inom hälso- och sjukvården bedömer kunna medföra allvarlig fara för patientens hälsa eller vård eller någon annans rättigheter.

Medborgargränssnittet ska realiseras så att patienten genom gränssnittet kan meddela sådana samtycken som avses i 11 § och sådana förbud som avses i 12 § samt förmedla or-



gandonationsförbud, livstestamenten och andra viljeyttringar som gäller hälso- och sjukvården. När gränssnittet realiserar ska det dessutom säkerställas att patientens integritetsskydd inte äventyras. Uppgifter om minderåriga patienter får utlämnas genom gränssnittet till patienten och till hans eller hennes vårdnadshavare eller någon annan laglig företrädare. Vid utlämning av uppgifterna ska det som i 9 § 2 mom. i lagen om patientens ställning och rättigheter föreskrivs om en minderårig patients rätt att förbjuda att uppgifter om hans eller hennes hälsotillstånd och vård ges till hans eller hennes vårdnadshavare eller någon annan laglig företrädare då beaktas. Åtkomsten till uppgifter genom medborgargränssnittet påverkar inte patientens rätt till insyn enligt personuppgiftslagen.

Genom förordning av social- och hälsovårdsministeriet får närmare bestämmelser utfärdas om innehållet i de uppgifter som gäller åtkomst till information, genomförande och uppföljning av vård och om anslutningen av uppgifterna till medborgargränssnittet samt om hur uppgifterna visas över medborgargränssnittet och hur rätten till åtkomst till uppgifter genomförs i fråga om vårdnadshavaren till eller en laglig företrädare för en minderårig patient.

5 a kap.

Väsentliga krav på informationssystemen och hur kraven verifieras

19 a §

Väsentliga krav

Informationssystem som används för behandling av klient- och patientuppgifter inom socialvården samt hälso- och sjukvården ska uppfylla väsentliga krav på interoperabilitet, informationssäkerhet, dataskydd och funktionalitet.

Ett informationssystem uppfyller de väsentliga kraven då det har planerats och tillverkats samt fungerar i enlighet med de lagar som gäller informationssäkerhet och dataskydd och de bestämmelser som utfärdats med stöd av lagarna samt följer nationella föreskrifter om interoperabilitet. De väsent-

liga kraven på funktionalitet uppfylls om informationssystemet är lämpligt för sitt ändamål och det med systemet går att utföra de funktioner som krävs i lagar och med stöd av dem utfärdade bestämmelser vid behandlingen av klient- och patientuppgifter, om behandlingen överensstämmer med sitt syfte och om informationssystemets kapacitet är den som tillverkaren meddelat. Kraven ska uppfyllas såväl vid användningen av informationssystemet självständigt som tillsammans med andra informationssystem som är avsedda att anslutas till det.

Institutet för hälsa och välfärd får vid behov meddela närmare föreskrifter om innehållet i de väsentliga kraven. Innan föreskrifterna meddelas ska Institutet för hälsa och välfärd höra delegationen för elektronisk informationsadministration inom social- och hälsovården. Dessutom får Folkpensionsanstalten utfärda föreskrifter om de förfaranden som ska iakttas vid verifieringen av interoperabiliteten i fråga om sådana informationssystem som ska kopplas till hälso- och sjukvårdens riksomfattande informationssystemtjänster, nedan *hälsoarkivstjänster*, som avses i denna lag eller i lagen om elektroniska recept.

19 b §

Klassificering

Social- och hälsovårdens informationssystem indelas enligt användningsändamål och egenskaper i klasserna A och B. Till klass A hör de hälsoarkivstjänster som förvaltas av Folkpensionsanstalten samt de informationssystem som är avsedda att anslutas till hälsoarkivstjänsterna antingen direkt eller via en teknisk förmedlingstjänst. Till klass A hör också den förmedlingsservice som avses i 3 § 6 punkten. Övriga informationssystem hör till klass B.

Om det är oklart vilken klass ett informationssystem hör till ska Institutet för hälsa och välfärd besluta om vilken klass informationssystemet hör till.

Institutet för hälsa och välfärd får meddela närmare föreskrifter om klassificeringen av informationssystem.

19 c §

Allmänna skyldigheter för tillverkare av informationssystem

Tillverkaren ansvarar för planeringen, tillverkningen och klassificeringen av informationssystem för social- och hälsovården, oberoende av om åtgärderna utförs av tillverkaren själv eller av någon annan för dennes räkning.

I samband med informationssystemet ska tillverkaren ge systemanvändarna sådana uppgifter och anvisningar om informationssystemets ibruktagande, användning för produktion och underhåll som de behöver för systemets interoperabilitet, informationssäkerhet, dataskydd och funktionalitet. De uppgifter och anvisningar som följer med informationssystemet ska finnas på finska, svenska eller engelska. De uppgifter och anvisningar som är avsedda för social- och hälsovårdspersonal som använder informationssystemet ska dock finnas på finska och svenska.

Dessutom ska tillverkaren ha ett kvalitetssystem som tillämpas på planeringen och tillverkningen av informationssystemet.

19 d §

Verifiering av överensstämmelse med kraven

Överensstämmelse med kraven för informationssystem som hör till klass A ska verifieras med en utredning av tillverkaren om att systemet uppfyller alla krav på funktionalitet utifrån godkänd samtestning och överensstämmelseintyg av ett bedömningsorgan för informationssäkerhet.

Överensstämmelse med kraven för informationssystem som hör till klass B ska verifieras genom tillverkarens skriftliga utredning om att systemet uppfyller de väsentliga kraven enligt 19 a § om det har installerats och underhållits på behörigt sätt och används för avsett ändamål.

Institutet för hälsa och välfärd får meddela närmare föreskrifter om de förfaranden som ska iakttas vid verifieringen av överensstämmelse med kraven och om innehållet i utredningen.

19 e §

Samtestning

Ett informationssystem som hör till klass A ska vara interoperabelt med de riksomfattande informationssystemtjänsterna och de övriga informationssystemen som är anslutna till dem. Interoperabiliteten ska visas vid en samtestning som utförs av Folkpensionsanstalten. En förutsättning för samtestning är att tillverkaren av informationssystemet lämnar Folkpensionsanstalten en redogörelse för hur kraven på informationssystemets funktionalitet har genomförts och testats. Tidpunkten för och genomförandet av samtestningen ska avtalas med Folkpensionsanstalten.

Ett informationssystem av klass A som har tagits i användning för produktion ska delta i de samtestningar för andra informationssystem som är avsedda att anslutas till de riksomfattande informationssystemtjänsterna för att säkerställa att informationssystemen är interoperabla. Folkpensionsanstalten beslutar vilka informationssystem som ska delta i samtestningen. Tillverkarna av de informationssystem som deltar i samtestningen svarar själva för de kostnader som samtestningen föranleder.

Med avvikelse från 1 mom. utförs ingen separat samtestning av de centrala informationssystem som Folkpensionsanstalten förvaltar.

19 f §

Ibruktagande av informationssystem

Informationssystem som hör till klass A får tas i användning för produktion och anslutas till hälsoarkivstjänsterna när ett bedömningsorgan för informationssäkerhet har utfärdat ett överensstämmelseintyg för systemet. Informationssystem som hör till klass B får tas i användning för produktion efter det att tillverkaren av systemet har lämnat den skriftliga utredning som avses i 19 d §.

Tillverkaren ska underrätta Tillstånds- och tillsynsverket för social- och hälsovården om informationssystem som ska tas i användning för produktion. Av anmälan ska informa-

tionssystemets tillverkare och användningsändamål framgå. Dessutom ska tillverkaren göra en anmälan om informationssystem som inte längre används för produktion. Tillstånds- och tillsynsverket ska föra ett offentligt register över de informationssystem för social- och hälsovården som har anmälts till verket.

Tillstånds- och tillsynsverket för social- och hälsovården får meddela närmare föreskrifter om innehållet i anmälan och vilka uppgifter som ska antecknas i registret.

19 g §

Uppföljning efter ibruktagandet

Tillverkaren ska genom ett uppdaterat och systematiskt förfarande följa upp och utvärdera de erfarenheter som fås av informationssystemet under den tid det används för produktion. Anmälan om betydande avvikelser från de väsentliga kraven för informationssystemet ska göras till alla tillhandahållare av tjänster som använder systemet. Dessutom ska bedömningsorganet för informationssäkerhet och Tillstånds- och tillsynsverket för social- och hälsovården underrättas om betydande avvikelser i fråga om informationssystem som hör till klass A.

Tillverkaren av informationssystemet ska dessutom ge akt på förändringar i de väsentliga kraven som ställs på informationssystem och justera systemen i enlighet med förändringarna. Bedömningsorganet för informationssäkerhet ska underrättas om ändringar i informationssystem som hör till klass A. Överensstämmelseintyget ska förnyas om betydande ändringar har gjorts i informationssystemet eller om de väsentliga kraven har förändrats.

Tillverkaren ska bevara uppgifter om överensstämmelse med kraven och övriga uppgifter som tillsynen kräver i minst fem år efter det att informationssystemet inte längre används för produktion.

Institutet för hälsa och välfärd får meddela närmare föreskrifter om de i 1 mom. avsedda betydande avvikelserna och hur anmälningar om sådana ska göras.

5 b kap.

Tillhandahållare av tjänster samt egenkontroll

19 h §

Plan för egenkontroll

Tillhandahållare av socialvårdstjänster och tillhandahållare av hälso- och sjukvårdstjänster ska utarbeta en plan för egenkontroll med tanke på informationssäkerheten, dataskyddet och användningen av informationssystemen. Av planen ska det framgå hur följande frågor som anknyter till användningen av systemen säkerställs:

1) de som använder informationssystemen har den utbildning och erfarenhet som användningen kräver,

2) i samband med informationssystemen finns behövliga bruksanvisningar för en korrekt användning av informationssystemen,

3) informationssystemen används enligt tillverkarens anvisningar,

4) informationssystemen underhålls och uppdateras enligt tillverkarens anvisningar,

5) miljön är lämplig för ändamålsenlig användning av informationssystemen som säkerställer informationssäkerheten och dataskyddet,

6) övriga anslutna informationssystem och andra system äventyrar inte informationssystemens prestanda eller egenskaper när det gäller informationssäkerhet och dataskydd, samt

7) informationssystemen installeras, underhålls och uppdateras endast av personer med den yrkesskicklighet och kompetens som krävs.

Om en tillhandahållare av tjänster har anslutit sig som användare av hälsoarkivstjänsterna ska det av planen för egenkontroll också framgå hur man har tillgodosett kraven på en informationssäker användning av dessa riksomfattande tjänster. Dessutom ska den som producerar förmedlingsservice enligt 3 § 6 punkten upprätta en plan för egenkontroll för förmedlingsservicen och Folkpensionsanstalten ska upprätta en plan för de hälsoarkivstjänster som den sköter.

Tillhandahållare av tjänster, producenter

av förmedlingsservice och Folkpensionsanstalten ska följa upp att planen för egenkontroll genomförs.

Institutet för hälsa och välfärd får vid behov meddela närmare föreskrifter om de i 1 och 2 mom. avsedda utredningar och krav som ska tas in i planen för egenkontroll.

19 i §

Meddelande om avvikelser

Om en tillhandahållare av socialvårdstjänster och en tillhandahållare av hälso- och sjukvårdstjänster konstaterar betydande avvikelser när det gäller tillgodoseendet av de väsentliga kraven på ett informationssystem, ska denne underrätta informationssystemets tillverkare om saken. Om en avvikelse kan innebära en betydande risk för patientsäkerheten, informationssäkerheten eller dataskyddet ska också Tillstånds- och tillsynsverket för social- och hälsovården underrättas.

5 c kap.

Bedömning av informationssystemens överensstämmelse

19 j §

Godkännande av bedömningsorgan för informationssäkerhet

På godkännandet av och verksamheten vid ett bedömningsorgan för informationssäkerhet tillämpas i övrigt vad som föreskrivs i lagen om bedömningsorgan för informationssäkerhet.

19 k §

Bedömning av informationssystemen

Överensstämmelsen av de informationssystem inom social- och hälsovården som hör till klass A ska bedömas i enlighet med denna lag och lagen om bedömningsorgan för informationssäkerhet. I bedömningen av informationssäkerheten enligt denna lag ingår emellertid varken bedömning eller inspektion av vare sig tillverkarens eller användarens verksamhetsställten. Bedömningen av överens-

stämmelse görs på ansökan av informationssystemets tillverkare.

Om ett informationssystem som hör till klass A uppfyller förutsättningarna för överensstämmelse med kraven och Folkpensionsanstalten på basis av samtestning har gett ett positivt yttrande om uppfyllelsen av kraven på interoperabilitet, ska bedömningsorganet för informationssäkerhet utifrån sin bedömning av överensstämmelsen med kraven ge tillverkaren ett överensstämmelseintyg och en tillhörande kontrollrapport. Överensstämmelseintyget är giltigt i högst fem år. Den tid som intyget är i kraft kan förlängas med högst fem år i sänder. Bedömningsorganet för informationssäkerhet får avkräva tillverkaren alla uppgifter som behövs för bedömningen i syfte att upprätta överensstämmelseintyget och hålla det i kraft. På utfärdande av intyget tillämpas i övrigt vad som föreskrivs i 9 § i lagen om bedömningsorgan för informationssäkerhet.

Bedömningsorganet för informationssäkerhet ska vid behov, med iakttagande av hemfriden, göra inspektioner och bedömningar för att säkerställa att tillverkaren i sitt utvecklingsarbete tillämpar förfaranden som säkerställer informationssystemets överensstämmelse med kraven, och ge tillverkaren en utvärderingsrapport. Bedömningsorganet för informationssäkerhet ska beakta resultaten av de bedömnings- och granskningsåtgärder som gjorts under produktionstiden för informationssystemet.

19 l §

Återkallelse av överensstämmelseintyg

Om bedömningsorganet för informationssäkerhet konstaterar att ett informationssystem inte har uppfyllt eller inte längre uppfyller de krav som föreskrivs i eller med stöd av denna lag eller att ett överensstämmelseintyg av någon annan orsak inte borde ha beviljats, ska organet uppmana tillverkaren av informationssystemet att avhjälpa bristerna. Bedömningsorganet får återkalla intyget för viss tid eller helt och hållet eller bevilja intyget med begränsningar, om inte tillverkaren avhjälper bristerna inom den tid som organet satt ut. När tidsfristens längd bestäms ska det beak-

tas att en skälig tid behövs för att ändra informationssystemet.

19 m §

Anmälningsskyldighet för bedömningsorgan för informationssäkerhet

Ett bedömningsorgan för informationssäkerhet ska underrätta Tillstånds- och tillsynsverket för social- och hälsovården samt Folkpensionsanstalten om alla överensstämmelseintyg som har utfärdats, ändrats eller kompletterats eller som har återkallats för viss tid eller helt och hållet eller förvägrats. Dessutom ska bedömningsorganet för informationssäkerhet på begäran ge Tillstånds- och tillsynsverket för social- och hälsovården all behövlig ytterligare information i ärendet.

20 §

Styrning, övervakning och uppföljning

Tillhandahållare av socialvårdstjänster och av hälso- och sjukvårdstjänster, Folkpensionsanstalten, Tillstånds- och tillsynsverket för social- och hälsovården och Befolkningsregistercentralen ska följa och övervaka att det dataskydd och den datasäkerhet som hänför sig till deras service förverkligas. Om någon har behandlat klientuppgifter i strid med lagen, ska den behöriga tillhandahållaren av tjänster samt Folkpensionsanstalten på eget initiativ vidta behövliga åtgärder. För uppföljningen och övervakningen har tillhandahållaren av tjänster rätt att få logguppgifter för sina egna patientregister från Folkpensionsanstalten samt logguppgifter i anslutning till behandlingen av uppgifter i patientens informationshanteringstjänst som avses i 14 a §, till den del som anställda hos tillhandahållaren har haft åtkomst till och behandlat uppgifter i patientens informationshanteringstjänst.

Den ansvariga föreståndaren för en verksamhetsenhet för socialvård eller hälso- och sjukvård ska meddela skriftliga instruktioner om hur klientuppgifterna ska behandlas och om de förfaringsätt som ska iakttas samt se till att personalen har tillräcklig sakkunskap och kompetens för behandlingen av klient-

uppgifter. Den ansvariga föreståndaren ska också se till att den plan för egenkontroll som avses i 19 h § utarbetas och iakttas. Dessutom ska varje tillhandahållare av tjänster och Folkpensionsanstalten ha en dataskyddsansvarig för uppföljnings- och övervakningsuppgifter.

20 a §

Tillsyn och inspektioner av informationssystem

Tillstånds- och tillsynsverket för social- och hälsovården har till uppgift att övervaka och främja informationssystemens överensstämmelse med kraven.

Tillstånds- och tillsynsverket för social- och hälsovården har rätt att utföra inspektioner som krävs för tillsynen. För att utföra en inspektion har en inspektör rätt att få tillträde till alla lokaler där det bedrivs verksamhet som avses i denna lag eller där det förvaras uppgifter som är viktiga för tillsynen över efterlevnaden av denna lag. Inspektioner får dock inte utföras i utrymmen som används för boende av permanent natur. Under en inspektion ska dessutom iakttas vad som i 39 § 1 mom. i förvaltningslagen (434/2003) föreskrivs om genomförande av inspektion.

Vid en inspektion ska alla handlingar som inspektören ber om och som behövs för inspektionen läggas fram. På inspektörens begäran ska dessutom kopior av de handlingar som behövs för inspektionen överlämnas till inspektören utan avgift.

Inspektionerna ska protokollföras och en kopia av protokollet ska sändas till den som saken gäller inom 30 dagar. Inspektionen anses avslutad när en kopia av inspektionsprotokollet har delgetts den som saken gäller. Tillstånds- och tillsynsverket för social- och hälsovården ska bevara inspektionsprotokollet i tio år efter att inspektionen utförts.

20 b §

Rätt att anlita utomstående sakkunniga

Tillstånds- och tillsynsverket för social- och hälsovården har rätt att anlita utomstående sakkunniga för bedömning av informa-

tionssystemens överensstämmelse med kraven. Utomstående sakkunniga får delta i inspektioner som avses i denna lag samt undersöka och testa informationssystem. Utomstående sakkunniga ska ha den sakkunskap och kompetens som uppgifterna kräver.

Utomstående sakkunniga får inte utan tillstånd röja vad de på grund av sin ställning, sitt uppdrag eller sitt arbete har fått veta om en persons hälsotillstånd, sjukdom eller handikapp eller om social- eller hälsovårdsåtgärder som avser personen eller andra motsvarande omständigheter. Tystnadsplikten kvarstår efter det att uppdraget har upphört. På utomstående sakkunniga som utför uppgifter enligt denna lag tillämpas förvaltningslagens bestämmelser om tjänstemannajäv och bestämmelserna om straffrättsligt tjänsteansvar.

20 c §

Handräckning av polisen

Bestämmelser om handräckning av polisen finns i polislagen (872/2011).

20 d §

Föreläggande att fullgöra skyldigheter

Om någon tillverkare av informationssystem för social- eller hälsovården, tillhandahållare av socialvårdstjänster eller av hälso- och sjukvårdstjänster, producent av förmedlingsservice eller Folkpensionsanstalten har underlåtit att fullgöra sin skyldighet enligt denna lag, får Tillstånds- och tillsynsverket för social- och hälsovården utfärda ett föreläggande om att skyldigheten ska uppfyllas inom utsatt tid.

20 e §

Skyldigheter avseende informationssystem som är i bruk

När Tillstånds- och tillsynsverket för social- och hälsovården meddelar beslut om informationssystem med stöd av 20 d § får verket samtidigt ålägga tillverkaren att avhjälpa brister i informationssystem som används för produktion.

Om ett informationssystem kan äventyra

dataskyddet eller klient- eller patientsäkerheten och bristerna inte har avhjälpats inom den tidsfrist som Tillstånds- och tillsynsverket för social- och hälsovården har satt ut, får verket förbjuda användningen av informationssystemet till dess att den egenskap som äventyrar säkerheten har avhjälpats. Dessutom får Folkpensionsanstalten stänga förbindelser till hälso- och sjukvårdens riksomfattande informationssystemtjänster som den förvaltar, om ett anslutet informationssystem eller dess användarorganisation äventyrar den behöriga funktionen för de riksomfattande informationssystemtjänsterna.

Tillstånds- och tillsynsverket för social- och hälsovården får ålägga tillverkaren eller en befullmäktigad representant att inom den tid och på det sätt som verket bestämmer informera om beslut som gäller användningen av informationssystemet för produktion.

20 f §

Vite

Ett föreläggande som Tillstånds- och tillsynsverket för social- och hälsovården har meddelat eller ett beslut som verket har fattat med stöd av detta kapitel kan förenas med vite. Bestämmelser om vite finns i viteslagen (1113/1990).

20 g §

Rätt att få uppgifter

Tillstånds- och tillsynsverket för social- och hälsovården har rätt att avgiftsfritt och trots sekretessbestämmelserna för tillsynen över social- och hälsovårdens informationssystem få nödvändiga uppgifter av statliga och kommunala myndigheter samt av fysiska och juridiska personer som omfattas av denna lag eller de bestämmelser och beslut om social- och hälsovårdens informationssystem som utfärdats med stöd av lagen.

20 h §

Ändringssökande

Beslut som Tillstånds- och tillsynsverket för social- och hälsovården har fattat med

stöd av denna lag får överklagas hos förvaltningsdomstolen enligt vad som föreskrivs i förvaltningsprocesslagen (586/1996). Ett beslut av förvaltningsdomstolen får överklagas genom besvär hos högsta förvaltningsdomstolen, om högsta förvaltningsdomstolen beviljar besvärstillstånd.

Ett beslut som Tillstånds- och tillsynsverket för social- och hälsovården meddelat i samband med en inspektion får inte överklagas genom besvär. Omprövning av beslutet får begäras hos Tillstånds- och tillsynsverket för social- och hälsovården inom 30 dagar från det att inspektionen avslutats. Till beslutet ska fogas anvisningar om begäran om omprövning hos verket. Åtgärderna i beslutet ska vidtas trots begäran om omprövning. Beslut som Tillstånds- och tillsynsverket för social- och hälsovården har fattat med anledning av begäran om omprövning får överklagas genom besvär enligt 1 mom.

Beslut och förelägganden som Tillstånds- och tillsynsverket för social- och hälsovården har meddelat med stöd av denna lag ska iakttagas även om de överklagats, om inte besvärsmyndigheten bestämmer något annat.

22 §

Avgifter

Användningen av de riksomfattande informationssystemtjänster som avses i 14 § och som administreras av Folkpensionsanstalten och Befolkningsregistercentralen är avgiftsbelagd för tillhandahållare av tjänster. Den kommunala social- och hälsovårdens avgifter tas ut per sjukvårdsdistrikt hos samkommunen för sjukvårdsdistriktet. De avgifter som Folkpensionsanstalten tar ut bestäms trots 10 § i lagen om grunderna för avgifter till staten (150/1992) genom förordning av social- och hälsovårdsministeriet så att de motsvarar beloppet av kostnaderna för skötseln av tjänsterna. Avgifterna ska dessutom trygga likviditeten för Folkpensionsanstaltens servicefond. De avgifter som tas ut för Befolkningsregistercentralens prestationer bestäms i lagen om grunderna för avgifter till staten och med stöd av den.

Folkpensionsanstalten och Befolkningsregistercentralen ska årligen lämna social- och

hälsovårdsministeriet en utredning över det föregående årets kostnader och de faktorer som påverkat kostnaderna samt en bedömning av de totalkostnader som ligger till grund för användningsavgifterna för det följande året.

Tillverkare av informationssystem ansvarar för kostnaderna för verifieringen av överensstämmelse med kraven. Folkpensionsanstalten har rätt att ta ut en avgift för sådan samtestning som avses i 19 e § till sådant självkostnadsvärde som avses i 6 § 1 mom. i lagen om grunderna för avgifter till staten. Registrering och införande av en i 19 f § i denna lag avsedd anmälan i offentligt register hos Tillstånds- och tillsynsverket för social- och hälsovården är avgiftsbelagd. Avgifterna bestäms genom förordning av social- och hälsovårdsministeriet, med beaktande av vad som föreskrivs i och med stöd av lagen om grunderna för avgifter till staten. Bestämmelser om avgifter som gäller godkännande av bedömningsorgan för informationssäkerhet finns i 11 § i lagen om bedömningsorgan för informationssäkerhet.

Denna lag träder i kraft den 1 april 2014.

Åtgärder som krävs för verkställigheten av denna lag får vidtas innan lagen träder i kraft.

För informationssystem som hör till klass A krävs överensstämmelseintyg enligt denna lag senast den 1 januari 2015. Före det får ett informationssystem som saknar överensstämmelseintyg genom Folkpensionsanstaltens beslut anslutas till de riksomfattande informationssystemtjänsterna för en tid av högst två år. Om ett informationssystem som hör till klass A har anslutits till de riksomfattande informationssystemtjänsterna före denna lags ikraftträdande får informationssystemet användas utan överensstämmelseintyg till utgången av den tidsfrist som fastställts i samband med anslutningen. Om tidsfristen löper ut under 2014 får informationssystemet dock genom beslut av Folkpensionsanstalten användas i högst två år.

Informationssystem som hör till klass B ska uppfylla de väsentliga krav som anges i 19 a §, om de tas i bruk den 1 januari 2017 eller därefter. Ett informationssystem av klass B som tagits i bruk före det ska bringas i överensstämmelse med de väsentliga kra-

ven, om informationssystemet ändras väsentligt och det ändrade informationssystemet tas i bruk den 1 januari 2017 eller därefter. Om ett serviceavtal som avser ett informationssystem som hör till klass B har ingåtts före denna lags ikraftträdande och upphör den 1 januari 2017 eller därefter, ska informationssystemet emellertid ändras så att det överensstämmer med de väsentliga kraven räknat från det serviceavtalet upphör.

Folkpensionsanstalten ska genomföra den tjänst som avses i 14 § 1 mom. och som innebär att riksomfattande informationssystemtjänster kan användas med hjälp av internet och telekommunikationsnät senast den 1 januari 2017.

De som ska ha en plan för egenkontroll enligt 19 h § är

1) Folkpensionsanstalten samt tillhandahållare av tjänster och producenter av för-

medlingsservice som har anslutit sig till de riksomfattande informationssystemtjänsterna när denna lag träder i kraft, senast den 1 januari 2015,

2) de som efter ikraftträdandet av denna lag ansluter sig till de riksomfattande informationssystemtjänsterna för hälso- och sjukvården från och med anslutningen; om anslutningen sker senast den 1 januari 2015 ska planen dock finnas senast vid nämnda tidpunkt, och

3) andra tillhandahållare av tjänster som använder socialvårdens samt hälso- och sjukvårdens informationssystem senast den 1 april 2015.

Tillstånds- och tillsynsverket för social- och hälsovården ska ha ett sådant offentligt register över social- och hälsovårdens informationssystem som avses i 19 f § 2 mom. senast den 31 december 2016.

Helsingfors den 28 mars 2014

Republikens President

SAULI NIINISTÖ

Omsorgsminister *Susanna Huovinen*