Informationstjänster
Social- och hälsovårdsinformation och informationshantering 9.12.2021

FÖRESKRIFT OM VÄSENTLIGA KRAV PÅ FUNKTIONALITET OCH INFORMATIONSSÄKERHETKRAV HOS INFORMATIONSSYSTEM FÖR SOCIAL- OCH HÄLSOVÅRDEN

Bemyndigande

Lag om elektronisk behandling av kunduppgifter inom social- och hälsovården (784/2021, nedan lagen om kunduppgifter), 29 § 4 mom., 32 § 4 mom., 34 § 4 mom., 35 § 3 mom. och 9 § 2 mom.

Målgrupper

Producenter av informationssystemtjänster och tillverkare av informationssystem för social- och hälsovården
Producenter av Kanta-informationsförmedlingsservice
Tillhandahållare av social- och hälsovårdstjänster
Apoteken
Folkpensionsanstalten
Bedömningsorgan för informationssäkerhet
Mellanhänder

Giltighetstid

Föreskriften träder i kraft den 9 december 2021 och den gäller tills vidare.

Genom föreskrift 4/2021 upphävs de tidigare föreskrifterna THL 1/2015 och 2/2016, som också har inkluderat ämnesinnehåll i denna föreskrift (5/2021). Tidigare föreskrifter har utfärdats med stöd av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården 159/2007. Lag 159/2007 har upphävts genom lag 784/2021.

Innehåll

1 Föreskriftens syfte

Syftet med denna föreskrift är att precisera de väsentliga krav som ställs på informationssystem som är avsedda för behandling av klient- och patientuppgifter inom social- och hälsovården, så att deras ändamålsenliga funktion, kompabilitet och informationssäkerhet kan säkerställas.

2 Föreskriftens tillämpningsområde

Denna föreskrift gäller innehållet i de väsentliga kraven på informationssystem som behandlar klient- eller patientuppgifter inom social- och hälsovården (7 kap. i lagen om kunduppgifter, ”Väsentliga krav på informationssystem och välbefinnandeapplikationer”). Institutet för hälsa och välfärd (nedan THL) har med stöd av 34 § 4 mom. i lagen om kunduppgifter bemyndigats att meddela närmare föreskrifter om innehållet i de väsentliga kraven och om vilka väsentliga krav som ska uppfyllas i de informationssystem som används i olika tjänster, och med stöd av 35 § bemyndigats att meddela föreskrifter om de förfaranden som ska iakttas vid påvisande av överensstämmelse med kraven och om innehållet i den utredning som ska ges.

Denna föreskrift gäller

- informationssystem som behandlar klient- och patientuppgifter och som är avsedda att anslutas till de riksomfattande informationssystemtjänsterna (Kanta-tjänsterna) och andra informationssystem och tjänster tillhandahållna av mellanhänder som i fråga om sitt användningsändamål kräver certifiering (klass A1, A2 och A3) och

- andra system för social- och hälsovården vars användningsändamål är behandling av klient- och patientuppgifter (klass B).

Användningsändamålen för de väsentliga kraven i föreskriften:

- beskriva och kommunicera klient- eller patientdatasystemens eller delsystemens användningsändamål;

- sammanställa nationellt fastställda krav samt hitta och hänvisa till specifikationer som närmare beskriver kraven;

- förtydliga de krav som gås igenom vid FPA:s samtestning med Kanta-tjänsterna och dess olika testhelheter av informationssystem i klass A2 och A3 som ska anslutas till Kanta-tjänsterna;

- stöda systemtillverkarens egen testning av funktionaliteten innan tillverkaren ansöker om samtestning;

- gruppera de systemegenskaper som testas av tillverkarna av informationssystem och producenterna av informationssystemtjänster, vid FPA:s samtestning samt vid eventuella kundtester;

- beskriva informationssäkerhetskraven i anslutning till bedömning av informationssäkerheten för bedömningar av informationssäkerheten;

- gruppera och länka till krav och specifikationer som hänför sig till samma funktionella eller sakliga helheter;

- sammanställa de specifikationer som gäller vid olika tidpunkter för implementering av en viss funktion eller ett visst datainnehåll;
- ange obligatoriska krav för system avsedda för särskilda ändamål;
- förtydliga tidtabellerna och övergångstiderna för de obligatoriska kraven (till exempel i fråga om de övergångstider som fastställs i lagen om kunduppgifter och de specifikationer och väsentliga krav som gäller ett visst år);
- stöda beskrivningen och beaktandet av de väsentliga krav som ställs nationellt vid planering och implementering av informationssystem samt vid upphandling av informationssystem;
- beskriva egenskaperna hos olika delsystem i informationssystemhelheter och modulära informationssystem; samt
- förenhetliga de begrepp och krav som används i kraven på systemtillverkare, producenter av informationssystemtjänster deras användare och som grundar sig på författningar och nationella specifikationer.

3 Föreskriftens centrala innehåll och avgränsningar

Enligt lagen om kunduppgifter ska ett informationssystem som används vid behandling av klient- eller patientuppgifter uppfylla väsentliga krav på interoperabilitet, informationssäkerhet, dataskydd och funktionalitet. Tillverkaren av informationssystemet eller producenten av informationssystemtjänsten ansvarar för att informationssystemet uppfyller kraven.

I lagen om kunduppgifter föreskrivs också att de informationssystem som en tjänstetillhandahållare använder ska till sitt användningsändamål svara mot tjänstetillhandahållarens verksamhet och uppfylla de väsentliga krav som ställs på tjänstetillhandahållarens verksamhet. Denna föreskrift preciserar hur man säkerställer att de väsentliga kraven uppfylls i de informationssystem som en tjänstetillhandahållare använder.

Enligt lagen om kunduppgifter ska tillverkaren av ett informationssystem för social- och hälsovården eller producenten av en informationssystemtjänst påvisa att systemet eller tjänsten överensstämmer med kraven. Till påvisandet hör en utredning om att systemet uppfyller de väsentliga krav som motsvarar dess användningsändamål. Utredningen ges i enlighet med föreskrift 4/2021 och denna föreskrift.

Till denna föreskrift bifogas en nationellt enhetlig klassificering av väsentliga krav hos informationssystemen för social- och hälsovården (bilaga 2). Klassificeringen innehåller beskrivningar på övre nivå av väsentliga krav på de informationssystem som används för behandling av klient- och patientuppgifter inom social- och hälsovården. I föreskriften preciseras också vilka väsentliga krav som åtminstone ska implementeras eller uppfyllas hos system avsedda för olika ändamål (bilaga 3). I denna föreskrift preciseras dessutom de förfaranden som används vid beskrivning, verifiering och utnyttjande av väsentliga krav.

Föreskriften gäller både system som ansluts till Kanta-tjänsterna och andra system som behandlar klient- och patientuppgifter och som hör till klass A eller B. Flera av kraven och de specifikationer som ligger till grund för dem gäller system i klass A2 eller A3 som ansluts till Kanta-tjänsterna (se föreskrift 4/2021).

Termerna och avgränsningarna som används i föreskriften motsvarar termerna i föreskrift 4/2021.

Föreskriften och dess bilagor har beretts av experter från Institutet för hälsa och välfärd (THL), Folkpensionsanstalten (FPA), Tillstånds- och tillsynsverket för social- och hälsovården (Valvira), Social- och hälsovårdsministeriet (SHM), Transport- och kommunikationsverket (Traficom) samt utvecklingsprojekten för tillhandahållare av social- och hälsovårdstjänster. I föreskriften beaktas de utvecklingsbehov som har identifierats i samband med tillämpningen av tidigare författningar.

Innan denna föreskrift utfärdades har Institutet för hälsa och välfärd ordnat en remiss för att höra berörda intressentgrupper. Resultaten av hörandena har beaktats i föreskriften och dess bilagor.

4 Förhållande till andra föreskrifter, anvisningar och specifikationer

THL har meddelat en föreskrift om klassificering och certifiering av informationssystem för social- och hälsovården (THL:s föreskrift 4/2021: Föreskrift om klassificering och certifiering av informationssystem för social- och hälsovården). Denna föreskrift preciserar de krav som ska verifieras med de förfaranden som beskrivs i föreskrift 4/2021 och de förfaranden som ska användas för att anmäla och verifiera överensstämmelse med olika krav.

THL har meddelat den separata föreskriften 1/2021 om klienthandlingar inom socialvården och om de uppgifter som ska antecknas i dem.

I THL:s föreskrift 3/2021 beskrivs de utredningar och krav som ska ingå i den informationssäkerhetsplan som förutsätts av tillhandahållare av social- och hälsovårdstjänster, mellanhänder och FPA. I informationssäkerhetsplanen beskrivs hur tjänstetillhandahållaren för sin del säkerställer att de informationssystem som används för produktion av tjänster överensstämmer med kraven som en del av informationssäkerhetsplanen och egenkontrollen som sker via den.

Klassificeringen av väsentliga krav i bilaga 2 till denna föreskrift hänvisar till flera närmare specifikationer och anvisningar som beskriver detaljerade krav på funktionalitet och datainnehåll. Klassificeringen är avsedd att förtydliga och stöda utvecklingen, certifieringen, testningen, bedömningen av informationssäkerheten och upphandlingen av informationssystem och tjänster samt kommunikationen mellan olika parter. När föreskriften tillämpas fungerar klassificeringen också som ett register, genom vilket man kan hitta de viktigaste specifikationerna som beskriver de nationella kraven.

De väsentliga krav som beskrivs i föreskriften och dess bilagor ersätter de väsentliga krav som fastställts med stöd av den tidigare lagen om klientuppgifter samt föreskrifterna 1/2015 och 2/2016. En stor del av de väsentliga kraven är desamma som i tidigare föreskrifter.

Denna föreskrift tillämpas inte på informationssystem vars användningsändamål uteslutande är ändamål enligt föreskrift 1/2020, som utfärdats av Tillståndsmyndigheten för social- och hälsovårdsdata (Findata) (Krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer). Föreskriften i fråga tillämpas på alla de användningsändamål som föreskrivs i lagen om sekundär användning, för vilka det enligt lagen om sekundär användning behövs dataanvändningstillstånd. Dessa användningsändamål är vetenskaplig forskning, statistikföring, undervisning samt myndigheternas planerings- och utredningsuppgifter.

5 Väsentliga krav på funktionalitet

Väsentliga krav på funktionalitet gäller funktioner och datainnehåll i informationssystemen. Väsentliga krav på funktionalitet är de funktioner och datainnehåll som beskrivs i bilaga 2 till denna föreskrift (Klassificering av väsentliga krav) och som hänvisar till separata, närmare specifikationer. I dessa närmare specifikationer beskrivs också obligatoriska och frivilliga funktioner och uppgifter mer detaljerat.

Många av de väsentliga kraven på funktionalitet fokuserar i denna föreskrift på de funktioner och uppgifter som är centrala för informationssystem som ansluts direkt eller indirekt till Kanta-tjänsterna.

6 Väsentliga informationssäkerhetskrav

Väsentliga informationssäkerhetskrav gäller de egenskaper som implementeras i informationssystem och via vilka man uppfyller informationssäkerheten och dataskyddet samt de åtgärder som behövs för att planera, genomföra eller tillhandahålla ett informationssystem, ett delsystem eller en informationssystemtjänst. Väsentliga informationssäkerhetskrav är de informationssäkerhetskrav som beskrivs i bilaga 2 till denna föreskrift (Klassificering av väsentliga krav). En del av kraven hänvisar till separata, närmare specifikationer.

De krav som presenteras under ”Rubrik” och ”Förklaring” på fliken Informationssäkerhetskrav i klassificeringen av väsentliga krav är bindande krav. Uppfyllandet av varje krav ska verifieras som en del av bedömningen av informationssäkerhet i ett informationssystem som hör till klass A enligt det verifieringssätt som fastställts för kravet, om kravet är relevant för systemets användningsändamål. Verifieringen som en del av certifieringsprocessen sker i enlighet med föreskrift 4/2021.

Producenten av en informationssystemtjänst måste ta ställning till vilka av de väsentliga informationssäkerhetskraven i informationssystemets driftsmiljö som uppfylls via informationssystemet eller de därtill anslutna tjänsterna som tillhandahålls av producenten av informationssystemtjänsten och vilka av kraven i driftsmiljön som den tjänstetillhandahållare som använder informationssystemet ansvarar för (se kapitel 9). Krav som ingår i ett informationssystem eller i en tjänst som tillhandahålls av producenten av en informationssystemtjänst verifieras som en del av bedömningen av informationssäkerheten. Vid verifiering och certifiering förutsätts inte att tjänstetillhandahållarorganisationen deltar i verifieringen av de krav som ställs på driftsmiljön.

7 Minimikravprofiler

Minimikraven på ett informationssystem, ett delsystem eller en informationssystemhelhet för ett visst användningsändamål kan uttryckas med hjälp av en nationell minimikravprofil (profil). En profil innehåller en delgrupp av de funktioner och datainnehåll som beskrivits i klassificeringen av väsentliga krav. I bilagorna 3a–3g till föreskriften finns profiler som sammanställer nationella minimikrav för flera användningsändamål inom informationssystemen för social- och hälsovården. Varje bilaga innehåller en eller flera profiler.

De väsentliga kraven enligt en profil ska implementeras eller uppfyllas i ett informationssystem vars användningsändamål inkluderar det användningsändamål som beskrivs i profilen. Uppfyllandet av minimikraven enligt en profil är en förutsättning för att ett informationssystem eller en informationssystemhelhet som används för ett visst ändamål ska godkännas för att tas i användning för produktion av tjänster. Profilerna som bifogas till denna föreskrift är bindande.

Producenten av en informationssystemtjänst ska anmäla alla de nationella minimikravprofiler vars användningsändamål ingår i informationssystemet. Ett undantag är profiler vars beskrivning särskilt anger att profilen i fråga inte behöver anmälas separat om systemet uppfyller kraven för en annan (mer omfattande) profil.[1] Anmälan görs som en del av certifieringen av ett informationssystem i klass A och som en del av beskrivningen och

[1] När föreskrift 5/2021 träder i kraft är profil 3g1 (i bilaga 3g) en sådan profil vars krav man har tagit ställning till i alla profiler enligt bilagorna 3a–3f. I detta fall behöver inte profil 3g1 anges separat på systemblanketten om systemet uppfyller kraven för någon annan profil.

registreringen av användningsändamålet för ett informationssystem i klass A eller klass B i enlighet med föreskrift 4/2021 och med hjälp av systemblanketten i bilaga 4 till denna föreskrift;

1. när man ansöker om samtestning med FPA för ett system i klass A2 eller A3

2. när man ansöker om bedömning av informationssäkerheten för ett system i klass A1, A2 eller A3

3. när man registrerar ett system i klass B, A1, A2 eller A3 i Valviras register över informationssystem.

Ett informationssystem, ett delsystem eller en informationssystemhelhet kan uppfylla kraven för flera profiler. Väsentliga krav som är obligatoriska i de minimikravprofiler som motsvarar systemets användningsändamål ska ha implementerats i systemet och antecknats på systemblanketten.

Kraven enligt en viss profil kan uppfyllas med ett eller flera informationssystem eller delsystem. Då ska man i anmälningarna och vid certifieringarna beskriva tillsammans med vilka andra informationssystem eller delsystem informationssystemet eller informationssystemtjänsten uppfyller kraven enligt profilen, och vilka andra villkor det finns för att kraven ska uppfyllas.

Implementering eller uppfyllande av de krav som förutsätts av profilerna som ingår i systemets användningsändamål samt verifiering av dem vid samtestning eller bedömning av informationssäkerheten till den del kraven kan verifieras vid certifieringen, är en förutsättning för att certifieringen av informationssystem i klass A ska godkännas och för att de ska kunna tas i användning för produktion av tjänster.

I registret över informationssystem som förs av Valvira anges profilerna som ingår i användningsändamålet för varje informationssystem eller delsystem.

Om det är fråga om ett informationssystem i klass A förutsätter registreringen i Valviras register över informationssystem att de krav på interoperabilitet och informationssäkerhet som hänför sig till funktionerna enligt profilen har verifierats med godkänt resultat vid samtestning och bedömning av informationssäkerheten och att informationssystemet har fått ett informationssäkerhetsintyg. I system som hör till klass A ska överensstämmelse med kraven vid behov verifieras som ett led i certifieringen också när kraven uppfylls via andra informationssystem eller delsystem.

Det är också möjligt att utfärda separata föreskrifter om minimikraven för informationssystem avsedda för ett visst ändamål och att i dessa föreskrifter hänvisa till profiler som specificerats med hjälp av klassificeringen.

Användningen av profiler och hur de förhåller sig till väsentliga krav beskrivs också i bilaga 1.

8 Uppfyllandet av väsentliga krav/producenten av en informationssystemtjänst

För att påvisa att de väsentliga kraven uppfylls använder producenten av en informationssystemtjänst den systemblankett som finns i bilaga 4. Med blanketten anmäls uppgifter om ett informationssystem vid certifiering och registrering av system i enlighet med föreskrift 4/2021. Alla väsentliga krav som implementerats i ett informationssystem eller delsystem beskrivs på en systemblankett. Punkterna om informationssystem i detta kapitel kan också tillämpas på delsystem som kan certifieras som en del av en större informationssystemhelhet.

Ett informationssystem i **klass B** uppfyller de väsentliga krav som ställs på systemet när

1. producenten av en informationssystemtjänst har beskrivit informationssystemets användningsändamål, klassificerat systemet och bedömt systemets risknivå i enlighet med föreskrift 4/2021;

2. producenten av en informationssystemtjänst har specificerat på systemblanketten de profiler för de väsentliga kraven (bilaga 3) som motsvarar informationssystemets användningsändamål;

3. producenten av en informationssystemtjänst har antecknat på systemblanketten de funktioner i de väsentliga kraven som systemet omfattar;

4. producenten av en informationssystemtjänst har antecknat på systemblanketten det datainnehåll för de väsentliga kraven som behandlas i systemet och som uttrycker vilka uppgifter systemet producerar eller använder;

5. producenten av en informationssystemtjänst har på systemblanketten antecknat de informationssäkerhetskrav som ingår i de väsentliga kraven och som implementeras i systemet eller uppfylls via det;

6. de krav som antecknats i enlighet med punkterna 3–5 omfattar åtminstone kraven enligt de profiler som gäller systemet;

7. det i kraven enligt punkterna 3–5 på systemblanketten har antecknats a) de krav som systemet uppfyller med hjälp av andra informationssystem eller delsystem samt b) de krav som anknyter till betydande ändringar i systemet, om sådana krav finns;

8. tillverkaren av ett informationssystem eller producenten av en informationssystemtjänst *själv har testat och verifierat* att de väsentliga kraven i punkterna 3–7 fungerar i systemet.

Ett informationssystem i **klass A1** uppfyller de väsentliga krav som ställs på systemet när

9. villkoren för klass B (ovan) har uppfyllts;

10. de väsentliga informationssäkerhetskraven för systemet (punkt 5) har *implementerats, uppfyllts och dokumenterats* så att systemet kan genomgå en bedömning av informationssäkerheten och få ett intyg över godkänd bedömning av informationssäkerhet.

11. Förutsättningar för att ta i användning ett informationssystem i klass A1, A2 eller A3 för produktion av tjänster är att informationssäkerhetsintyget över de verifierade informationssäkerhetskraven som beskrivs ovan har utfärdats och att uppgifterna som motsvarar intyget finns i Valviras register över informationssystem (se även föreskrift 4/2021, kap. 9).

Ett informationssystem i **klass A2 eller A3** uppfyller de väsentliga krav som ställs på systemet när

11. villkoren för klass A1 (ovan) har uppfyllts;

12. man i fråga om det datainnehåll som behandlas (punkt 4) har antecknat på systemblanketten vilka uppgifter systemet producerar till Kanta-tjänsterna eller utnyttjar hos Kanta-tjänsterna;

13. de krav på systemets funktionalitet (funktioner och datainnehåll, punkterna 3–8) som gäller specifikationerna i anslutning till Kanta-tjänsterna har *implementerats, uppfyllts och dokumenterats* så att

systemet kan genomgå nödvändiga samtestningar med godkänt resultat enligt anvisningarna för FPA:s samtestning med Kanta-tjänsterna.

Anmälan av ovan nämnda omständigheter med hjälp av systemblanketten beskrivs i kapitel 2.3 i bilaga 1 till föreskrift 5/2021.

En förutsättning för att ta i användning ett informationssystem i klass A2 eller A3 för produktion av tjänster är att alla funktioner och datainnehåll i systemet som är anslutna till Kanta-tjänsterna och som är föremål för samtestning har samtestats med godkänt resultat (se även föreskrift 4/2021, kap. 9).

Överensstämmelsen med kraven för ett informationssystem som hör till klass A ska påvisas genom certifiering innan det tas i användning för produktion av tjänster. Ett informationssystem i klass A eller B som uppfyller de väsentliga kraven ska registreras i Valviras register över informationssystem. Processen för certifiering och registrering beskrivs i föreskrift 4/2021 och i bilaga 1 till denna föreskrift. Numreringen av ovannämnda förutsättningar motsvarar inte direkt skedena i certifierings- och registreringsprocessen.

Om ett system i klass A anmäls till förnyad bedömning av behovet av samtestning eller för bedömning av om systemet behöver en ny bedömning av informationssäkerheten, ska nya funktioner och datainnehåll och sådana som innehåller väsentliga ändringar antecknas tydligt i systemblanketten enligt bilaga 4.

En systemblankett enligt denna föreskrift samt den utredning och anmälan som lagen om kunduppgifter förutsätter ska göras oberoende av om systemet uppfyller minimikraven för en enda nationell profil. På systemblanketten antecknas också andra väsentliga krav än de som ingår i profilerna som har implementerats i systemet eller som uppfylls via systemet.

På systemblanketten som används vid certifieringen eller registreringen antecknas inte sådana systemegenskaper som är i planeringsstadiet eller som inte har implementerats i systemet.

Krav som uppfylls via integrationsgränssnitt eller andra system eller delsystem kan antecknas om uppfyllandet av dem kan verifieras som en del av certifieringen.

Producenten av en informationssystemtjänst ska i enlighet med 32 § ge akt på ändringar i väsentliga krav och göra justeringar i enlighet med ändringarna. Om ändringarna förutsätter en ny samtestning eller en ny bedömning av informationssäkerheten, ska dessa åtgärder vidtas innan den version av informationssystemet som innehåller ändringarna tas i användning för produktion av tjänster.

Producenten av en informationssystemtjänst ska åtminstone vid ansökan om förnyelse av informationssäkerhetsintyget kontrollera att informationssystemets egenskaper som ska anslutas till Kanta-tjänsterna har samtestats i enlighet med gällande specifikationer och specifikationsversioner samt kapitel 10 i föreskrift 4/2021.

Tjänstetillhandahållaren, FPA, bedömningsorganet, THL eller någon annan instans kan göra en anmälan till Valvira om informationssystemet inte uppfyller de väsentliga krav som ställs när systemet används för produktion av tjänster.

9 Uppfyllandet av väsentliga krav/tjänstetillhandahållare

Enligt 34 § i lagen om kunduppgifter och lagens ikraftträdande- och övergångsbestämmelser ska också de informationssystem som en tjänstetillhandahållare använder till sitt användningsändamål svara mot

tjänstetillhandahållarens verksamhet och uppfylla de väsentliga krav som ställs på tjänstetillhandahållarens verksamhet. De väsentliga kraven kan uppfyllas med en helhet som består av ett eller flera informationssystem eller delsystem.

Enligt 27 § i lagen om kunduppgifter och föreskrift 3/2021 ska en tjänstetillhandahållare i sin informationssäkerhetsplan beskriva de informationssystem som den använder för behandling av klient- och patientuppgifter.

Till den del det i tjänstetillhandahållarens verksamhet behövs informationssystem som används för de användningsändamål som beskrivs i de nationella minimikravprofilerna, ska tjänstetillhandahållaren säkerställa att de informationssystem eller delsystem som den använder i sin helhet uppfyller kraven i profilerna i fråga.

En tjänstetillhandahållare ska med iakttagande av tidsfristerna i lagen om kunduppgifter ansluta sig som användare av Kanta-tjänsterna. För att kunna ansluta sig måste tjänstetillhandahållaren ha ett informationssystem eller en informationssystemhelhet som uppfyller kraven för anslutning till Kanta-tjänsterna och som gör det möjligt att behandla och lagra de kunduppgifter som behövs i tjänstetillhandahållarens verksamhet. Informationssystemet som används för anslutning kan vara ett informationssystem som hör till klass A3 eller en helhet som består av olika informationssystem, där kraven relaterade till Kanta-tjänsterna uppfylls med hjälp av informationssystem eller delsystem som hör till åtminstone klass A2.

En tjänstetillhandahållare ska säkerställa att de informationssystem i klass A1, A2 eller A3 som den använder har certifierats med godkänt resultat, att systemens egenskaper som tas i användning för produktion av tjänster via Kanta-tjänsterna har samtestats med godkänt resultat i förhållande till gällande krav och att informationssäkerhetsintyget för dem är giltigt. Tjänstetillhandahållaren ska också i övrigt sträva efter att säkerställa att varje informationssystem som den använder uppfyller de väsentliga kraven för sitt användningsändamål. Tjänstetillhandahållaren ska utnyttja Valviras register över informationssystem samt upphandlings- och underhållsavtal med producenter av informationssystemtjänster för att säkerställa dessa omständigheter.

En tjänstetillhandahållare ska för sin del säkerställa att Valviras register innehåller aktuella uppgifter om de informationssystem i klass A1, A2, A3 eller B som används i tjänstetillhandahållarens verksamhet.

En tjänstetillhandahållare ska i sin egen verksamhet, när informationssystem tas i bruk och används för produktion av tjänster samt i verksamheten enligt informationssäkerhetsplanen, beakta de omständigheter som ska uppmärksammas beträffande de väsentliga kraven samt de observationer och förutsättningar som framkommit i certifieringen och som påverkar implementeringen av väsentliga krav i de system som tjänstetillhandahållaren använder.[2] Särskild uppmärksamhet ska fästas vid de preciseringar som publiceras via Valviras register över informationssystem för hur systemen uppfyller överensstämmelsen med kraven.

En tjänstetillhandahållare ska enligt 27 § i lagen om kunduppgifter som en del av sin informationssäkerhetsplan säkerställa att informationssystemets driftsmiljö är lämplig för en sådan ändamålsenlig användning av informationssystemen som säkerställer informationssäkerheten och dataskyddet. En del av kraven på driftsmiljön kan uppfyllas via det informationssystem som producenten av en informationssystemtjänst ansvarar för (se kapitel 6). Varje informationssystem ska uppfylla de väsentliga krav på driftsmiljön som producenten av en informationssystemtjänst ansvarar för. En tjänstetillhandahållare ska säkerställa att man har avtalat med

[2] Det kan till exempel vara fråga om ett informationssäkerhetskrav som för att bli uppfyllt förutsätter åtgärder i driftsmiljön för tjänstetillhandahållaren som använder systemet eller ett krav på funktionalitet som uppfylls via gränssnitten för systemintegration.

producenterna av informationssystemtjänster och eventuella andra parter om vilka krav på driftsmiljön som ska uppfyllas via respektive part

Om en tjänstetillhandahållare själv har rollen som tillverkare av ett informationssystem eller producent av en informationssystemtjänst, ska tjänstetillhandahållaren i fråga om det informationssystem som tjänstetillhandahållaren ansvarar för uppfylla de skyldigheter som författningarna ålägger tillverkaren av ett informationssystem eller producenten av en informationssystemtjänst, inklusive klassificering av systemet, uppfyllande av väsentliga krav, certifiering och registrering. Detta gäller även eventuella situationer där informationssystemet inte har en sådan utsedd ansvarig part som ansvarar för överensstämmelsen med kraven enligt lagen om kunduppgifter. Om en tjänstetillhandahållare som använder informationssystemet i dessa fall inte har avtalat om ansvaret för klassificeringen, de väsentliga kraven, registreringen och certifieringen av informationssystemet, ansvarar tjänstetillhandahållaren för dessa åtgärder.

10 Preciseringar av verifieringen av väsentliga krav

10.1 Bedömning av uppfyllandet av krav i system som inte ansluts till Kanta-tjänsterna

För system i klass B utförs ingen sådan samtestning eller bedömning av informationssäkerheten som hör till certifieringen. För system i klass A1 utförs ingen samtestning, men de genomgår en bedömning av informationssäkerheten.

Systemet i klass B eller A1 omfattas inte av de detaljerade kravspecifikationerna för informationssystem som ansluts direkt till Kanta-tjänsterna. De krav på behandling av klient- och patientuppgifter som härrör direkt från författningarna gäller även system i klass B och A1, liksom även system i klass A2 och A3. I klassificeringen av väsentliga krav (bilaga 2) specificeras krav som härrör direkt från de viktigaste författningarna som styr behandlingen av kunduppgifter och som man hänvisar till i de olika kraven. Specifikationerna och hänvisningarna i dessa krav avseende system som ansluts till Kanta-tjänsterna **gäller inte** system i klass B eller A1, om inte annat uttryckligen anges i specifikationsdokumentet eller hänvisningen. För system i klass B och A1 härrör innehållet i dessa krav direkt från de bestämmelser som hänvisas till i de olika kraven.

De krav som allmänt gäller behandlingen av klient- och patientuppgifter och som även gäller system i klass B och A1 har sammanställts i profilbilagan 3g till denna föreskrift. Dessa lagstadgade krav gäller alla system avsedda för behandling av klient- eller patientuppgifter, om inte en närmare systemprofil särskilt nämner att kravet inte gäller system enligt profilen i fråga. Om ett system i klass B eller A1 indirekt använder uppgifter i Kanta-tjänsterna eller producerar uppgifter som skickas till Kanta-tjänsterna, kan systemet också omfattas av kraven i profilbilaga 3b ”3b2 – Applikation som utnyttjar uppgifter som hämtas från Kanta-arkiveringstjänsten” eller ”3b4 – Applikation som producerar uppgifter som lämnas till Kanta-arkiveringstjänsten”.

Utöver de krav som ingår i ovannämnda profiler (3g1, 3b2, 3b4) ska producenten av en informationssystemtjänst i enlighet med kapitel 8 i systemblanketten anteckna även andra väsentliga krav enligt vilka funktioner, datainnehåll eller informationssäkerhetskrav har implementerats i informationssystemet.

10.2 Bedömning av uppfyllandet av kraven och verifieringssätten vid certifiering

I certifieringen av system i klass A (samtestning och bedömning av informationssäkerheten) bedöms varje krav som har implementerats i systemet och som omfattas av samtestning eller bedömning av informationssäkerheten. Bedömaren är FPA vid samtestning och bedömningsorganet vid bedömning av informationssäkerheten.

I fråga om ett enskilt krav kan den som bedömer kravet ta ställning till huruvida kravet uppfylls enligt följande:

- huruvida kravet är relevant i systemet
    - relevanta krav är åtminstone alla obligatoriska och rekommenderade väsentliga krav som anges i profiler som motsvarar systemets användningsändamål samt de väsentliga krav som har implementerats i systemet enligt anteckningarna på den systemblankett som producenten av en informationssystemtjänst har lämnat in;
    - om kravet endast delvis är relevant i fråga om det informationssystem eller delsystem som ska bedömas eller om det är nödvändigt att särskilt uppge att kravet inte är relevant i systemet (till exempel med beaktande av systemets användningsändamål och begränsningar av användningsändamålet), kan bedömaren göra en anteckning om detta i den rapport, det utlåtande eller det intyg som bedömningen ger upphov till, om saken behöver motiveras;

- avseende relevanta krav
    - kravet uppfylls helt (normal situation);
    - kravet uppfylls inte eller uppfylls endast delvis. Den del som inte uppfylls kompenseras på ett godtagbart sätt så att målet som eftersträvas med kravet uppnås, varvid kompensationssättet måste beskrivas;
    - kravet uppfylls inte;
    - vid behov en anteckning om verifieringssättet och hur uppfyllandet av kravet har verifierats, till exempel hänvisning till dokumentation, testrapport eller programvara

Ovannämnda uppgifter kan ingå i en detaljerad rapport om samtestning eller bedömning av informationssäkerheten.

De obligatoriska väsentliga kraven på systemets användningsändamål måste uppfyllas i de system som tas i användning för produktion av tjänster.

Om ett obligatoriskt väsentligt krav inte uppfylls kan bedömaren fastställa en tidsfrist för uppfyllandet av kravet innan testningen eller bedömningen av informationssäkerheten godkänns som en del av den pågående certifieringsprocessen.

Om ett relevant krav inte uppfylls, men dess mål kan uppnås med godtagbar kompensation, kan bedömaren fatta beslut om godkännande så att den godtagbara kompensationen anges i samtestningsutlåtandet eller informationssäkerhetsintyget samt i Valviras register. För att bedöma om kompensationen är godtagbar kan bedömaren kräva en riskbedömning och en beskrivning av kompensationen av producenten av en informationssystemtjänst. Kompensation är en åtgärd som vidtas i undantagsfall och det måste finnas en vägande grund för att godkänna åtgärden till exempel med tanke på klient- eller patientsäkerheten eller social- och hälsovårdstjänsternas funktion. Kompensationen får inte medföra olägenheter eller oskäliga krav eller kostnader för andra aktörer. Producenten av en informationssystemtjänst ska underrätta de tjänstetillhandahållare som använder systemet om godkända kompensationer.

Om ett obligatoriskt krav i anslutning till den minimikravprofil som systemet förutsätter inte uppfylls och kravet inte kan kompenseras på ett godtagbart sätt, uppfyller systemet inte profilens krav. Detta ska nämnas i testrapporten eller rapporten om bedömning av informationssäkerheten. I anmälan till Valviras register över informationssystem ska man inte uppge den profil vars krav på funktionalitet eller interoperabilitet systemet inte uppfyller. Då får systemet inte tas i användning för produktion av tjänster för användningsändamålet i fråga. Det kan dock användas för de ändamål vars krav har certifierats med godkänt resultat och anmälts. Då ska producenten av en informationssystemtjänst för sin del säkerställa att systemet inte används för ett användningsändamål vars krav systemet inte uppfyller. Ett begränsat användningsändamål ska nämnas i anmälan till Valviras register över informationssystem och producenten av en informationssystemtjänst ska underrätta de

tjänstetillhandahållare som använder systemet om det begränsade användningsändamålet. Begränsningen av användningsändamålet kan efter justeringar tas bort med en godkänd kompletterande certifiering.

Kompensationer och avvikelser från uppfyllandet av de obligatoriska kraven enligt profilerna antecknas i informationssäkerhetsintyget, om de hänför sig till informationssäkerhetskraven. Producenten av en informationssystemtjänst ska underrätta de tjänstetillhandahållare som eventuellt använder systemet om eventuella kompensationer och tidsfrister som tillsynsmyndigheten fastställt.

Om det vid certifieringen framgår att ett informationssystem som redan *används för produktion av tjänster* inte uppfyller ett obligatoriskt relevant krav, ska informationssystemet justeras eller kravet kompenseras på ett godtagbart sätt.

Valvira kan meddela ett föreläggande om att en skyldighet ska fullgöras inom utsatt tid (44 § i lagen om kunduppgifter). Tidsfristen kan också gälla en skyldighet i anslutning till certifieringen för producenten av en informationssystemtjänst eller tillverkaren, såsom justering eller kompensation. Tidsfristen kan gälla alla driftsmiljöer för ett system som används för produktion av tjänster (se även kapitel 10.4, punkt 6).

I Valviras register över informationssystem anges uppgifter om avvikelser, resultaten av samtestning och informationssäkerhetsintygets giltighet för informationssystem som används för produktion av tjänster. Via registret är det också möjligt att publicera information om andra omständigheter relaterade till användningen eller certifieringen av informationssystemet, såsom kompensationer eller begränsningar som ska beaktas i användningen av systemet.

Om bedömningen av uppfyllandet av ett krav förutsätter en mer precis tolkning av specifikationsdokumentet som ligger till grund för kravet, ska bedömaren vid behov försöka bekräfta tolkningen hos den part som ansvarar för specifikationsdokumentet, till exempel FPA eller THL. Den ansvariga parten ska publicera den preciserade tolkningen, i första hand i samband med det ursprungliga specifikationsdokumentet.

Producenten av en informationssystemtjänst ska förbereda sig för samtestning eller bedömning av informationssäkerheten så att de relevanta och icke-relevanta kraven har identifierats och så att man kan presentera det material som behövs om uppfyllandet av de relevanta kraven eller vidta nödvändiga verifieringsåtgärder.

Vid verifieringen av informationssäkerhetskraven används följande verifieringssätt:

V: validering eller teknisk inspektion, till exempel genomgång av en logg, meddelandeinstans eller en rapport från systemet;

testning där

TT: applikationen utvärderas genom att man (med testning av funktionaliteten) använder en egenskaps existens eller ändamålsenlighet som en del av bedömningen av informationssäkerheten;
HT: en teknisk informationssäkerhets- och sårbarhetstestning och bedömning av säkerhetsnivån genomförs som en del av bedömningen av informationssäkerheten.

D: genomgång av systemdokumentation eller andra systemrelaterade dokument;

(kompletterande): **H**: intervju som en del av bedömningen av informationssäkerheten, som kan fördjupa och komplettera bedömningen; en intervju är inte godtagbar som primär metod för kravverifiering av system i klass A.

Om det som ska bedömas är ett väsentligt informationssäkerhetskrav som har verifierats i informationssystemet med stöd av andra gällande författningar än lagen om kunduppgifter av en tredje part som godkänns i dessa författningar, ska kravet inte verifieras på nytt. Detta förutsätter att den verifiering som utförts av en tredje part är i kraft och att producenten av en informationssystemtjänst lägger fram den dokumentation som behövs för verifieringen och godkännandet. Av dokumentationen ska framgå åtminstone tillräckligt specificerade uppgifter om föremålet för det verifierade kravet, den författning som verifieringen grundar sig på, det verifierade kravet jämte källhänvisningar och hur kravet motsvarar det väsentliga kravet i fråga, en anteckning om att kravet verifierats med godkänt resultat, uppgifter om den tredje part som verifierat kravet samt verifieringens giltighet. Exempel på krav som verifierats med stöd av andra författningar är externa auditeringar av kvalitetssystemet för tillverkare av medicintekniska produkter.

Vid verifieringen av krav ska man använda ett verifieringssätt som är tillräckligt för att verifiera varje krav eller kravpunkt. Vilket verifieringssätt och vilken verifieringsnivå som är tillräcklig beror på kravet, systemets detaljerade klassificering, omfattning och användningsändamål (bland annat med beaktande av innehållets omfattning och den risknivå som avgörs av typen av uppgifter som behandlas). Verifieringssättet och verifieringsnivån för olika krav beskrivs också i bilagorna 1, 2 och 3 till denna föreskrift. För varje informationssäkerhetskrav anges i bilaga 2 och vid behov i profilerna de verifieringsnivåer som ska användas för system som placeras i de olika klasserna eller som är avsedda för olika ändamål.

Särskilt vid tekniska informationssäkerhets- och sårbarhetstester är det en rekommendation att ett lämpligt allmänt ramverk för informationssäkerhetstestning tillämpas, såsom OWASP ASVS eller MASVS, i den mån kraven motsvarar eller är förenliga med informationssäkerhetskraven i bilaga 2. 10.3 Versionshantering av krav och specifikationer

Ett system som används för produktion av tjänster eller som certifieras ska uppfylla alla väsentliga krav som implementerats i systemet i enlighet med gällande specifikationer, om specifikationerna innehåller krav som motsvarar systemets klass och användningsändamål.

THL eller FPA publicerar uppgifter om gällande specifikationer och specifikationsversioner, och med stöd av vilka versioner överensstämmelsen med kraven ska verifieras. FPA publicerar aktuella uppgifter om vilka specifikationer och specifikationsversioner som förutsätts i Kanta-tjänsternas produktionsmiljö och i samtestningen med Kanta-gränssnitten. I ett informationssystem som hör till klass A2 eller A3 ska systemimplementeringen, samtestningen och ett positivt utlåtande grunda sig på sådana väsentliga krav, specifikationer och specifikationsversioner som vid respektive tidpunkt förutsätts av ett system som ansluts till Kanta-tjänsterna. I Kanta-tjänsterna är det möjligt att stöda flera versioner av specifikationerna med olika funktioner och datainnehåll.

Om det i samband med att THL:s eller FPA:s nya specifikationer eller specifikationsversioner träder i kraft krävs att en tidigare systemimplementering ändras på ett sätt som kräver ny certifiering, anger THL eller FPA detta i samband med att specifikationerna publiceras. Om en ny certifiering eller en ny bedömning av certifieringsbehovet krävs, ska dessa åtgärder genomföras inom den tidsfrist som anges i föreskriften eller i anslutning till specifikationen. Om dessa åtgärder eller tidsfrister inte krävs är också implementeringar enligt tidigare specifikationsversioner godtagbara vid testning och i användning för produktion av tjänster.

FPA eller THL publicerar information om vilka specifikationsversioner som ska tas bort eller ersättas och fram till vilken tidpunkt man kan godkänna implementeringar enligt en specifikationsversion som ska tas bort eller ersättas

vid certifieringen av system i klass A och i produktionsmiljön för Kanta-tjänsterna. Kraven som gäller stöd för olika versioner av strukturer och uppgifter i klienthandlingarna inom socialvården beskrivs i THL:s föreskrift 1/2021.

Anmälningar om systemändringar i förhållande till certifiering av system i klass A behandlas i bilaga 2 till föreskrift 4/2021.

Mer information om utnyttjandet av specifikationer och hur de förhåller sig till väsentliga krav finns i bilaga 1 till föreskriften.

10.4 Avvikelser från överensstämmelsen med kraven

I informationssystem som används för produktion av tjänster är följande avvikelser betydande:

1. Avvikelser som medför risker för patient- eller klientsäkerheten;

2. Avvikelser som medför betydande risker för dataskyddet, informationssäkerheten eller verksamheten inom social- och hälsovårdstjänsterna;

3. Avvikelser från väsentliga krav i ett informationssystem som används för produktion av tjänster som medför betydande eller långvariga återverkningar eller ytterligare avvikelser för flera tjänstetillhandahållare eller flera andra informationssystem;

4. Avvikelser som orsakar omfattande störningar i uppgifternas riktighet, integritet eller interoperabilitet (särskilt via Kanta-tjänsterna);

5. Ett föråldrat överensstämmelseintyg eller intyg över bedömning av informationssäkerhet för ett system som används för produktion av tjänster, särskilt om förnyandet av intyget drar ut på tiden av orsaker som beror på tillverkaren av ett informationssystem eller producenten av en informationssystemtjänst;

6. Egenskaperna hos ett system som används för produktion av tjänster grundar sig på en föråldrad specifikationsversion, vars giltighetstid har löpt ut eller vars stöd i Kanta-tjänsterna har tagits bort eller håller på att tas bort så att systemet inte har kunnat eller inte kan övergå till implementering enligt gällande krav inom den tidsfrist som fastställts i författningar eller av tillsynsmyndigheten;

7. De tidsfrister för justeringar i systemet som fastställts i författningar eller av myndigheter har inte iakttagits, särskilt om försummelsen upprepas;

8. Andra avvikelser som tillsynsmyndigheten (såsom Valvira, RFV eller Dataombudsmannens byrå) konstaterat är betydande avvikelser.

Betydande avvikelser ska anmälas i enlighet med 41 § och 32 § i lagen om kunduppgifter. Tillverkaren av ett informationssystem, producenten av en informationssystemtjänst, en mellanhand eller en tjänstetillhandahållare som berörs av en betydande avvikelse ska vidta åtgärder för att rätta till avvikelsen. Valvira publicerar information om avvikelser som rör informationssystem i registret över informationssystem. Valvira styr och främjar överensstämmelsen med kraven i enlighet med lagen om kunduppgifter. Valvira kan bland annat utföra inspektioner (40 §), meddela ett föreläggande att fullgöra en skyldighet eller avhjälpa brister (44 § och 45 §), meddela användningsförbud (45 §) samt förena ett föreläggande eller beslut som det meddelat med vite (49 §).

Om man i certifieringsprocessen upptäcker en sådan avvikelse från de väsentliga kraven som skulle leda till en betydande avvikelse i användningen för produktion av tjänster, kan certifieringen inte slutföras med godkänt resultat innan den omständighet som orsakar avvikelsen har justerats eller innan de fellägen som beror på avvikelsen har förhindrats på annat sätt

Krav som inte uppfylls eller uppfylls på ett bristfälligt sätt kan medföra justeringsbehov innan samtestningen eller bedömningen av informationssäkerheten godkänns, enligt beskrivningen i avsnitt 10.2.

Om ett informationssystem som används för produktion av tjänster inte uppfyller de gällande, obligatoriska väsentliga kraven på systemet eller om dess överensstämmelse med kraven har föråldrats, ska producenten av en informationssystemtjänst underrätta Valvira och de tjänstetillhandahållare som använder informationssystemet om saken. Valvira och de tjänstetillhandahållare som använder informationssystemet ska i enlighet med 32 § underrättas om betydande avvikelser. Om avvikelsen beror på informationssystemet eller på den verksamhet som producenten av en informationssystemtjänst eller tillverkaren bedriver, ska producenten av informationssystemtjänsten bedöma den risk som avvikelserna medför och planera nödvändiga justeringar eller fortsatta åtgärder utifrån riskbedömningen. Om det är fråga om ett krav som har verifierats i certifieringen och som inte uppfylls på grund av ändringar i systemet, ska nödvändiga ändringsanmälningar göras enligt bilaga 2 till föreskrift 4/2021. Dessa åtgärder ska vidtas utöver vad som annars föreskrivs i 32 § och 41 § i lagen om kunduppgifter om uppföljning efter ibruktagandet av ett informationssystem och om underrättelse om avvikelser.

Ett informationssystem eller delsystem ska fungera korrekt i fråga om de funktioner och datainnehåll som implementerats i systemet. Det kan konstateras att ett system avviker från de väsentliga kraven om det uppenbart inte fungerar korrekt. Detta förutsätter inte att kravet på korrekthet särskilt omnämns i de väsentliga kraven eller i de specifikationer som de hänvisar till.

11 Handledning och rådgivning

Mer information om tillämpningen av denna föreskrift och certifieringsprocessen i förhållande till de väsentliga krav som ställs på informationssystem finns i bilaga 1. Mer information om de väsentliga kraven och certifieringsprocessen finns på THL:s på webbplatsen och på webbplatsen Kanta.fi.

Institutet för hälsa och välfärd ger på begäran råd och handledning om tillämpningen av denna föreskrift.

12 Ikraftträdande och övergångsbestämmelser

Denna föreskrift träder i kraft den 1 månadxx 2021 och gäller tills vidare.

I föreskrift 4/2021 beskrivs övergångsbestämmelserna med tanke på verifieringen av överensstämmelsen med kraven i tidigare certifierade system och systemens giltighet.

Informationssystemprofiler för socialvården som motsvarar kraven i lagen om kunduppgifter publiceras i början av 2022. De klientdatasystem som ansluts till Klientdataarkivet för socialvården ska certifieras enligt dessa profiler senast när organisationen enligt lagen om kunduppgifter är skyldig att ansluta sig till den riksomfattande arkiveringstjänsten. Före dess kan klientdatasystemen certifieras med informationssystemprofiler enligt fas 2 av Klientdataarkivet för socialvården. Certifikat för profilerna enligt fas 1 beviljas inte längre.

Avseende ikraftträdandet av kraven i föreskrifterna ska *datumet då föreskriften träder i kraft* beaktas. Från och med detta datum tillämpas föreskriften och dess bilagor med de preciseringar som anges här och de *datum som anges i övergångsbestämmelserna för föreskrift 4/2021*. Genom dessa uttrycks giltighetstiden och kontinuiteten för åtgärder

och krav som vidtagits innan föreskrifterna trädde i kraft, till exempel giltighetstiden för de tidigare certifierade systemens överensstämmelse med kraven eller förfarandena för certifieringsprocesser som pågår när föreskriften träder i kraft.

I fråga om genomförandet av profiler och krav, certifieringen och anmälningarna till Valviras register över informationssystem ska dessutom följande tidpunkter för ikraftträdandet av kraven beaktas:

1. *Datumet då profilen träder i kraft vid certifieringar och i anmälningar*, som anges i bilagan till föreskrift 5/2021. Från och med detta datum ska kraven i profilen senast tillämpas vid certifieringen av system (samtestning och bedömning av informationssäkerheten) och i anmälningar till Valviras register över informationssystem, om systemets användningsändamål överensstämmer med profilen.

2. *Datumet som visas för ett enskilt krav i profilen* och som beskriver tidpunkten då kravet har trätt i kraft eller träder i kraft i de informationssystem som används i produktion enligt profilen. I ett system som används för produktion enligt profilen ska kravet implementeras eller uppfyllas senast vid denna tidpunkt. Om det står ”rekommenderas” vid kravet är det en rekommendation att kravet implementeras i ett system som överensstämmer med profilen, men det är inte en förutsättning för att systemet ska godkännas för användning för produktion av tjänster. Om det står ”giltigt” eller ett passerat datum vid kravet, baseras kravet på tidigare gällande bestämmelser och det ska vara implementerat i alla system som används för produktion av tjänster och som omfattas av kravet. Kravens giltighetstid kan också preciseras enligt krav- eller systemklass. Eventuella preciseringar anges vid varje krav i respektive profil. Vid certifieringen iakttas tidsfristerna i punkt 1 så att de krav som gäller åtgärder för samtestning eller bedömning av informationssäkerheten har verifierats och en motsvarande anmälan har sänts till Valviras register över informationssystem innan systemet eller systemversionen tas i användning för produktion av tjänster. Vid certifieringen ska kraven beaktas i testningen och produktionsanvändningen enligt gällande och kommande specifikationer, såsom beskrivs i avsnitt 10.3.

Om ett system uppfyller kraven för flera olika profiler och ett krav har olika ikraftträdandedatum i olika profiler, ska kravet implementeras i systemet enligt den datum som infaller först.

Föreskrifter som utfärdas senare kan ersätta eller komplettera denna föreskrift. Separata föreskrifter kan utfärdas om de väsentliga krav eller profiler som särskilt förutsätts för olika social- och hälsovårdstjänster. Klassificeringen av väsentliga krav kan kompletteras utan att föreskriften ändras vid tidpunkter som meddelas separat. Profiler som baseras på föreskriften och klassificeringen kan publiceras för nya ändamål, och de kan göras bindande genom nya föreskrifter.

Underskrifter

Pekka Rissanen
t.f. Direktör för informationstjänsterna

Jarmo Kärki
Enhetschef

Bilagor

Bilaga 1. Tillämpningsanvisningar för väsentliga krav på informationssystem för social- och hälsovården

Bilaga 2. Klassificering av väsentliga krav.

Bilaga 3a. Profiler: Profiler för e-recept

Bilaga 3b. Profiler: Minimikrav på system som ska anslutas till Kanta-arkiveringstjänsterna

Bilaga 3c. Profiler: Profiler för Patientdataarkivet

Bilaga 3d. Profiler: Profiler för Klientdataarkivet för socialvården (publiceras senare)

Bilaga 3e. Profiler: Profiler för bilddiagnostik

Bilaga 3f. Profiler: Profiler för intyg

Bilaga 3g. Profiler: Minimikrav på system avsedda för behandling av klient- eller patientuppgifter (inkl. klass B eller A1)

Bilaga 4: Systemblankett

Sändlista

Tillhandahållare av social- och hälsovårdstjänster
Mellanhänder
Folkpensionsanstalten
Tillverkare av klient- och patientdatasystem samt producenter av informationssystemtjänster för social- och hälsovården
Producenter av informationsförvaltningstjänster och ICT-tjänster för social- och hälsovården
Kompetenscentrum inom det sociala området
Social- och hälsovårdsministeriet
Finlands Kommunförbund rf
Valvira
FIMEA
Finansministeriet
Arbets- och näringsministeriet
Befolkningsregistercentralen
Dataombudsmannens byrå
Regionförvaltningsverken

Denna föreskrift finns på webbadressen

https://www.finlex.fi/fi/viranomaiset/normi/561001/ (FINLEX ® – Myndigheternas föreskriftssamlingar: Institutet för hälsa och välfärd) samt

på registratorskontoret vid Institutet för hälsa och välfärd samt

på webbadressen https://thl.fi/sv/web/informationshantering-inom-social-och-halsovarden/foreskrifter-och-specifikationer/foreskrifter