Informationstjänster
Social- och hälsovårdsinformation och informationshantering 09.12.2021

ANMÄLAN OM ÄNDRINGAR I INFORMATIONSSYSTEM FÖR SOCIAL- OCH HÄLSOVÅRDEN SOM HÖR TILL KLASS A

I denna bilaga beskrivs de ändringar i ett informationssystem som tidigare samtestats eller godkänts vid en bedömning av informationssäkerheten som ska anmälas till FPA och bedömningsorganet för informationssäkerhet. Bilagan sammanställer och preciserar förfarandena vid ändringar av informationssystem enligt lagen om kunduppgifter och föreskrift 4/2021.

Bakgrund och grunder

Tillverkaren av ett informationssystem eller producenten av en informationssystemtjänst ansvarar i enlighet med lagen om kunduppgifter och föreskrifterna 4/2021 och 5/2021 för att informationssystemet för social- och hälsovården överensstämmer med kraven och för de relaterade skyldigheterna avseende samtestning och bedömning av informationssäkerhet som avses i lagen om kunduppgifter.

I lagen om kunduppgifter föreskrivs att betydande ändringar i informationssystem som hör till klass A ska anmälas till *bedömningsorganet för informationssäkerhet*. Ett nytt intyg över bedömning av informationssäkerhet ska utfärdas om det görs betydande ändringar i informationssystemet eller om de väsentliga kraven på systemet ändras.

Interoperabiliteten mellan de uppgifter i klient- och patientdatasystemen som registreras i Kanta-tjänsterna och andra klient- och patientdatasystem ska påvisas i en samtestning som utförs tillsammans med FPA. Kravet på interoperabilitet gäller också situationer där betydande ändringar görs i systemen. Därför föreskrivs i lagen om kunduppgifter att betydande ändringar i informationssystemen också ska anmälas till *FPA*.

En förutsättning för samtestning och bedömning av informationssäkerheten är tillverkarens redogörelse för hur kraven på informationssystemets funktion har implementerats och testats. I redogörelsen används en systemblankett enligt bilaga 4 till föreskrift 5/2021.

Om informationssystemen eller specifikationerna ändras kan man förenkla förfarandena för ny testning eller ny bedömning genom att begränsa ändringarna till vissa funktioner eller innehåll. Till exempel förutsätter implementering av en ny handlingstyp eller ett nytt strukturerat innehåll i systemet inte nödvändigtvis att alla funktioner i anslutning till informationsförmedling testas på nytt

Denna bilaga grundar sig på THL:s anvisning 2/2018, som utfärdats med stöd av tidigare författningar och som ersätts av denna bilaga. Innehållet i bilagan har beretts i myndighetssamarbete (THL, FPA, Valvira, Transport- och kommunikationsverket, SHM, bedömningsorgan för informationssäkerhet) utifrån enkäter som dessa instanser fått samt erfarenheter från certifieringsprocessen. Termerna som används i bilagan, såsom tillverkare och producent av en informationssystemtjänst, motsvarar termerna i lagen om kunduppgifter och i föreskrift 4/2021.

Förfarandet vid anmälan om ändringar

Producenten av en informationssystemtjänst ska anmäla betydande ändringar i system som hör till klass A1, A2 eller A3 till FPA och bedömningsorganet för informationssäkerhet i enlighet med denna bilaga. På basis av anmälan bedömer FPA eller bedömningsorganet för informationssäkerhet om ändringarna förutsätter en ny samtestning eller en sådan ny bedömning av informationssäkerheten som medför att ett nytt intyg över bedömning av informationssäkerhet ska utfärdas för informationssystemet eller ett delsystem.

Om den producent av informationssystemtjänster som ansvarar för kraven är någon annan än tillverkaren, ska tillverkaren och producenten av informationssystemtjänsten sinsemellan komma överens om vem som ansvarar för certifieringsförfarandena vid systemändringar och för anmälan av ändringar i systemet.

När producenten av en informationssystemtjänst byts ut måste man se till att kraven på systemet och dess uppdateringar fortfarande uppfylls och att detta finns dokumenterat.

Ändringsanmälan ska åtföljas av en systemblankett som fyllts i enligt THL:s föreskrifter 4/2021 och 5/2021 (Föreskrift 5/2021, bilaga 4). Blanketten ska lämnas in till FPA när man gör en ändringsanmälan till FPA för bedömning av behovet av samtestning. Blanketten ska också lämnas in tillsammans med ändringsanmälan till bedömningsorganet för informationssäkerhet för att organet ska kunna avgöra om det är nödvändigt att göra en ny bedömning av informationssäkerheten för systemet. *På systemblanketten ska man med anteckningarna i föreskrift 5/2021 anteckna funktioner, datainnehåll och informationssäkerhetskrav som är nya eller som innehåller betydande ändringar och som implementerats i systemet eller som uppfylls via systemet. Nya och ändrade väsentliga krav som implementerats i systemet måste tydligt skilja sig från de väsentliga krav som tidigare verifierats i systemet.*

I samband med anmälningar enligt denna bilaga ska uppgifterna om informationssystemet vid behov uppdateras även i Valviras register över informationssystem, om de tidigare anmälda uppgifterna ändras eller kompletteras. Anmälan till Valvira ska också göras om att en sådan version av ett informationssystem som är avsedd att användas för produktion av tjänster inte längre stöds (lagen om kunduppgifter, 30 §).

FPA och bedömningsorganet för informationssäkerhet kan ge närmare anvisningar om de blanketter och kontaktkanaler som ska användas vid ändringsanmälningar samt om man redan i samband med ändringsanmälan kan lämna även andra uppgifter som behövs för certifieringsprocessen till exempel i situationer där det är klart att en ny samtestning eller bedömning av informationssäkerheten behövs.

Om denna bilaga inte innehåller något svar på om det behövs en bedömning av behovet av en ny samtestning, kan man få råd via FPA:s Kanta-tjänster eller THL. Man kan fråga bedömningsorganet eller THL om behovet av en ny bedömning av informationssäkerheten om de regler som beskrivs i bilagan inte är tillämpliga.

Betydande ändringar

Betydande ändringar i ett informationssystem som hör till klass A2 eller A3 ska anmälas till FPA, som bedömer behovet av en ny samtestning av informationssystemet eller behovet av en kompletterande samtestning. Betydande ändringar i ett informationssystem som hör till klass A1 ska inte anmälas till FPA.

Om ett informationssystem övergår från klass A1 eller klass B till klass A2 eller A3, inleds en samtestning med FPA på motsvarande sätt som när man ansöker om samtestning för ett nytt system.

Betydande ändringar i ett informationssystem som hör till klass A1, A2 eller A3 ska anmälas till bedömningsorganet för informationssäkerhet, som bedömer om det är nödvändigt att göra en ny bedömning av informationssäkerheten för informationssystemet.

Om ett informationssystem övergår från klass B till klass A1, A2 eller A3, inleds tillsammans med bedömningsorganet för informationssäkerhet en bedömning av informationssäkerheten på motsvarande sätt som när man ansöker om bedömning av informationssäkerheten för ett nytt system.

De ändringar som beskrivs nedan är exempel på ändringar som förutsätter en anmälan till FPA:s Kanta-tjänster för bedömning av behovet av samtestning samt en anmälan till bedömningsorganet för informationssäkerhet för att bedömningsorganet ska kunna besluta om det behövs en ny bedömning av informationssäkerheten för systemet.

1. I systemet implementeras funktioner på basis av de nationella specifikationerna, och i dessa specifikationer eller i den tillhörande publikationsplanen nämns att ibruktagandet av en specifikation förutsätter en ny testning eller en ny bedömning av informationssäkerheten.

2. Systemets användargrupp eller anslutningsmodell förändras väsentligt i samband med en ny version, till exempel utökas användargruppen från professionella användare till att även omfatta klienter eller patienter inom social- och hälsovårdstjänsterna, eller så börjar systemet användas förutom av privata serviceproducenter även av offentliga serviceproducenter eller tvärtom.

3. Systemet ansluts till en Kanta-tjänst, som det inte tidigare har varit anslutet till, exempelvis förutom receptcentret även patientdataarkivet, förutom patientdataarkivet även klientdataarkivet för socialvården eller datalagret för egna uppgifter på Mina Kanta-sidor, eller förutom klientdataarkivet för socialvården även patientdataarkivet.

4. Systemets användargränssnitt eller funktion förnyas i betydande grad eller så görs betydande ändringar i dem. Sådana ändringar ska anmälas om ändringarna också kan påverka riktigheten hos de uppgifter eller handlingar som skickas till eller hämtas från Kanta-tjänsterna, funktionen hos Kanta-gränssnitten eller meddelandestrukturerna eller sättet på vilket informationssäkerhetskraven uppfylls.

5. Systemet ansluts direkt till Kanta-tjänsterna när det tidigare har varit anslutet till Kanta-tjänsterna via informationsförmedlingsservice för kunduppgifter eller via ett system som förmedlar uppgifter från Kanta-tjänsterna.

6. Tillsynsmyndigheten, till exempel Valvira, kräver en bedömning av behovet att testa systemet eller en ny version av det på nytt eller en bedömning av om det är nödvändigt att göra en ny bedömning av informationssäkerheten för systemet.

7. Tillverkaren av informationssystemet eller producenten av informationssystemtjänsten gör betydande ändringar i dokumentationsarrangemangen i anslutning till bedömningskraven för informationssäkerheten eller organiseringen av systemets utvecklingsarbete (till exempel betydande förändringar i affärsverksamheten såsom en företagsfusion eller ett företagsförvärv, byte av utvecklingsteamet som producerat systemet).

8. De väsentliga kraven på system X har samtestats med godkänt resultat eller godkänts i en bedömning av informationssäkerheten via system eller produkt Y, och system Y ändras så att ändringen kan påverka hur de väsentliga kraven uppfylls i system X.

9. Betydande brister eller fel som påverkar patient- eller klientsäkerheten påträffas i systemet. I fråga om betydande fel ska man särskilt se till att underrätta tillsynsmyndigheten (Valvira) och systemanvändarna.

Betydande ändringar som förutsätter anmälan till FPA:s Kanta-tjänster för bedömning av behovet av samtestning, men som inte förutsätter anmälan till bedömningsorganet för informationssäkerhet är till exempel följande typer av ändringar:

10. I systemet görs ändringar som påverkar Kanta-gränssnittet, de Kanta-serviceförfrågningar som systemet använder eller meddelande- eller dokumentstrukturerna som används i dessa.

Betydande ändringar som förutsätter anmälan till bedömningsorganet för informationssäkerhet, men som inte förutsätter anmälan till FPA:s Kanta-tjänster för bedömning av behovet av samtestning är till exempel följande typer av ändringar:

11. Informationssystemets användningsändamål ökar avsevärt till exempel från en enskild tjänsteproducent till ett stort område, eller så stiger informationssystemets risknivå från basnivå till hög nivå på grund av ändringar i systemet eller andra omständigheter som påverkar risknivån. Risknivån fastställs enligt föreskrift 4/2021.

12. I drifts- eller prestationsmiljön för ett system som producenten av en informationssystemtjänst ansvarar för görs betydande ändringar som påverkar hur de väsentliga kraven på informationssäkerhet i driftsmiljön uppfylls. Ändringen kan till exempel vara sådan att systemet eller en av dess viktiga delkomponenter överförs från miljön för producenten av en social- och hälsovårdstjänst eller producenten av en informationssystemtjänst till en extern producent av plattforms- eller programvarutjänster. Anmälningsbehovet gäller inte installation av ett godkänt system som genomgått en bedömning av informationssäkerheten med godkänt resultat i en ny kundmiljö där kraven uppfylls på motsvarande nivå och med motsvarande förfaranden som i tidigare driftsmiljöer. I de nya bedömningarna av informationssäkerheten bör man dock gå igenom om systemet har installerats i sådana nya driftsmiljöer där riskerna avviker från de tidigare.

13. Betydande brister eller fel som påverkar informationssäkerheten påträffas i systemet och korrigeringen av dessa måste säkerställas genom en bedömning av informationssäkerheten. I fråga om betydande fel är det särskilt viktigt att de anmäls till tillsynsmyndigheten (i synnerhet Valvira) och systemanvändarna.

Systemet behöver inte anmälas för bedömning av behovet av en ny bedömning av informationssäkerheten eller behovet av en ny samtestning i följande situationer. Även i dessa situationer måste man dock se till att Valviras register över informationssystem samt FPA:s Kanta-tjänster och bedömningsorganet för informationssäkerhet har aktuella uppgifter om produktnamnen på de system som används i produktion och om systemens tillverkare:

14. Ett system som tidigare testats eller som genomgått en bedömning av informationssäkerheten med godkänt resultat förses med ett nytt innehåll eller en ny funktion som inte påverkar Kanta-gränssnitten eller uppfyllandet av informationssäkerhetskraven, till exempel att en ny statusvy för avdelningens bäddplatser införs i ett sjukhussystem eller att en ny funktion för att visa påminnelser för användarna införs i ett klientdatasystem inom socialvården.

15. Systemets försäljningsnamn eller produktnamn ändras, men inga betydande ändringar görs i systemet som påverkar Kanta-gränssnitten, informationssäkerhetskraven eller funktionen. Det är tillåtet att uppdatera intyget över bedömning av informationssäkerhet med systemets nya produktnamn så att namnen på alla versioner av systemet som är i produktion framgår av intyget och intygets giltighetstid förblir oförändrad.

16. Företagets namn eller FO-nummer ändras, men ändringen påverkar inte företagets produkter eller informationssystem.

17. Kontaktpersonen för eller kontaktuppgifterna till tillverkaren eller producenten av en informationssystemtjänst ändras vid bedömning av informationssäkerheten eller samtestning.