Informationsförmedlare
Information och styrning av informationshanteringen 20.2.2024

FÖRESKRIFT OM REDOGÖRELSER OCH KRAV SOM SKA TAS IN I INFORMATIONSSÄKERHETSPLANEN

Bestämmelser om bemyndigande

Lag om behandling av kunduppgifter inom social- och hälsovården (703/2023) 77 § 3 mom.

Målgrupper

Tjänstetillhandahållare inom social- och hälsovården
Apotek
Mellanhänder
Folkpensionsanstalten (FPA)

Ikraftträdande

Denna föreskrift träder i kraft den 22 februari 2024 och gäller tills vidare.

Denna föreskrift ersätter Institutet för hälsa och välfärds (THL) tidigare föreskrift THL 3/2021 om redogörelser och krav som ska tas in i informationssäkerhetsplanen. Lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023) upphäver lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (784/2021), som gett fullmakt att utfärda den tidigare föreskriften. De författningar på lägre nivå som utfärdats med stöd av lagen om klientuppgifter upphävs.

Innehåll

1 Föreskriftens syfte och tillämpningsområde

THL:s föreskrift 3/2024 grundar sig på 77 § och 78 § i lagen om behandling av kunduppgifter inom social- och hälsovården (703/2023, nedan lagen om kunduppgifter).

THL har med stöd av 77 § 3 mom. i lagen om kunduppgifter bemyndigats att meddela närmare föreskrifter om de redogörelser och krav som enligt i 1 och 2 mom. ska tas in i informationssäkerhetsplanen och om verifiering av informationssäkerheten. I föreskriften beskrivs närmare vad som utgör säker digital eller icke-digital behandling av kunduppgifter inom social- och hälsovården.

Föreskriften om redogörelser och krav som ska tas in i informationssäkerhetsplanen gäller tjänstetillhandahållare inom social- och hälsovården, apotek, mellanhänder och Folkpensionsanstalten, som ska utarbeta en informationssäkerhetsplan med tanke på informationssäkerheten, dataskyddet och användningen av informationssystemen.

Med hjälp av informationssäkerhetsplanen sammanställs informationssäkerhetsrutinerna hos aktörerna inom social- och hälsovården. De informationssäkerhetsplaner som tjänstetillhandahållare, apotek, mellanhänder och FPA utarbetar ska innehålla redogörelser för hur kraven som hänför sig till behandlingen av klient- och patientuppgifter samt informationssystemen säkerställs i enlighet med 77 § 1 mom. punkterna 1–9 i lagen om kunduppgifter.

De aktörer som är skyldiga att utarbeta en informationssäkerhetsplan, dvs. målgrupperna för denna föreskrift, benämns i denna föreskrift och i bilagan till föreskriften med det allmänna namnet *objekt för egenkontroll av informationssäkerheten*.

Syftet med föreskriften är inte att ställa upp exakta krav för alla enskilda informationssäkerhetsrutiner. Organisationerna inom social- och hälsovården ser mycket olika ut, från enpersonsföretag till privata och offentliga organisationer med flera tusen personer. Det väsentliga är att fastställa hur de krav som hänför sig till behandlingen av kunduppgifterna och informationssystemen säkerställs i praktiken hos objektet för egenkontroll av informationssäkerheten, i enlighet med 77 § 1 mom. 1–9 punkten i lagen om kunduppgifter och denna föreskrift 3/2024 från THL.

Objektet för egenkontroll av informationssäkerheten har en skyldighet att agera i enlighet med sin informationssäkerhetsplan, regelbundet underhålla och granska sin plan samt aktivt följa upp genomförandet av planen. Det handlar om kontinuerlig och regelbunden riskhantering och att säkerställa att ändamålsenliga rutiner för informationssäkerhet och användning av kunduppgifter har införts och genomförs.

Föreskriften åtföljs av en mall för en informationssäkerhetsplan, dvs. en dokumentmall som fungerar som exempel och är avsedd som stöd för att utarbeta en informationssäkerhetsplan för objekt för egenkontroll av informationssäkerheten. Dokumentmallens struktur är informativ och vägledande, dvs. den underlättar och styr utarbetandet av planen.

2 Definitioner

Centrala begrepp i denna föreskrift och definitionerna av dem:

- **Kunduppgift** (3 § 1 mom. 6 punkten):
    - patientuppgifter samt klientuppgifter inom socialvården
- **Objekt för egenkontroll av informationssäkerheten**
    - De aktörer som är skyldiga att utarbeta en informationssäkerhetsplan, dvs. tjänstetillhandahållare inom social- och hälsovården, apotek, mellanhänder och Folkpensionsanstalten (FPA), benämns i denna föreskrift och i bilagan till föreskriften med det allmänna namnet objekt för egenkontroll av informationssäkerheten.
- **Personal**
    - Personer, inklusive inhyrd personal, som behandlar kunduppgifter eller deltar i behandlingen av kunduppgifter i den organisation som är objekt för egenkontroll av informationssäkerheten.
- **Tjänstetillhandahållare** (3 § 1 mom. 11 punkten[1]).
- **Apotek** (3 § 1 mom. 12 punkten i lagen om kunduppgifter):
    - ett sådant apotek som avses i 38 § 1 punkten i läkemedelslagen (395/1987).
- **Välbefinnandeapplikation** (3 § 1 mom. 18 punkten i lagen om kunduppgifter):
    - en applikation i anslutning till informationsresursen för egna uppgifter med vilken uppgifter om välbefinnande behandlas, samt en applikation till vilken personen kan få sina kunduppgifter från den riksomfattande informationsresursen för kunduppgifter, receptcentret och informationshanteringstjänsten.
- **Informationssystem** (3 § 1 mom. 19 punkten i lagen om kunduppgifter):
    - en programvara eller ett system eller delsystem som det i enlighet med de egenskaper som har planerats av tillverkaren är meningen att använda för elektronisk behandling av kundhandlingar, för registrering av handlingarna i de riksomfattande informationssystemtjänsterna eller för anslutning till de riksomfattande informationssystemtjänsterna eller med vars hjälp en yrkesutbildad person inom social- eller hälsovården kan använda uppgifter om välbefinnande.

[1] https://www.finlex.fi/sv/laki/alkup/2023/20230703

- **Producent av en informationssystemtjänst** (3 § 1 mom.) 20 punkten i lagen om kunduppgifter):

    - den som för en tjänstetillhandahållare tillhandahåller eller genomför ett i 3 § 1 mom. 19 punkten avsett informationssystem och som i egenskap av informationssystemets tillverkare, för tillverkarens räkning eller för en eller flera tillverkares del ansvarar för de krav som ställs på informationssystemet.

- **Tillverkare av ett informationssystem** (3 § 1 mom. 21 punkten i lagen om kunduppgifter):

    - den som ansvarar för planeringen och tillverkningen av ett informationssystem för social- och hälsovården.

- **Mellanhand** (3 § 1 mom. 22 punkten i lagen om kunduppgifter):

    - en tjänsteleverantör som en tjänstetillhandahållare anlitar vid produktionen av informationssystemtjänster, genomförandet av informationssystemens tekniska eller fysiska miljö eller anslutningen till de riksomfattande informationssystemtjänsterna och som i denna roll i samband med underhåll eller annars har en möjlighet att se okrypterade kunduppgifter.

- **Certifiering** (3 § 1 mom. 23 punkten i lagen om kunduppgifter):

    - ett förfarande genom vilket det verifieras att informationssystem och välbefinnandeapplikationer uppfyller de väsentliga krav som ställs på dem för att de ska få användas för produktion. Verifieringen av kraven för system som hör till klass A görs genom en bedömning av informationssäkerheten och vid behov genom samtestning. Anteckningar om en godkänd certifiering av systemet görs i tillsynsmyndighetens register (i enlighet med THL:s föreskrift 4/2024).

- **Tillsynsmyndighet** (97 § 3 mom. i lagen om kunduppgifter):

    - Dataombudsmannen, Säkerhets- och utvecklingscentret för läkemedelsområdet (Fimea), Tillstånds- och tillsynsverket för social- och hälsovården (Valvira) samt regionförvaltningsverket (AVI), som inom sitt verksamhetsområde styr och övervakar efterlevnaden av lagen om kunduppgifter i enlighet med sin behörighet.

- **Kanta-tjänsterna** (65 § 1 mom. i lagen om kunduppgifter)

    - De riksomfattande informationssystemtjänster inom social- och hälsovården som ordnas och upprätthålls av Folkpensionsanstalten.

- **Informationssystemets driftmiljö**:

    - en teknisk, organisatorisk och fysisk miljö där en eller flera tjänstetillhandahållare eller apotek använder informationssystemet eller delsystemet vid produktion av social- och hälsovårdstjänster och vid behandling av kunduppgifter. Driftmiljön omfattar bland annat terminaler, servrar, datorer, operativsystem och systemprogramvara, kommunikationsnät samt administrations- och informationssäkerhetsrutiner som inte är en del av informationssystemet.

3 Ansvar för säkerställande av informationssäkerheten och ändamålsenlig behandling av kunduppgifter

Objektet för egenkontroll av informationssäkerheten ska se till att de krav som ingår i informationssäkerhetsplanen uppfylls i samtliga av dess egna serviceenheter och i all verksamhet som bedrivs av andra tjänstetillhandahållare, inklusive eventuella underleverantörer, som deltar i produktionen eller genomförandet av tjänster för egenkontrollobjektets räkning. Alla ovan beskrivna enheters och underleverantörers ansvar ska framgå av redogörelserna i informationssäkerhetsplanen.

Ansvaret för alla parter som är involverade i behandlingen av kunduppgifter ska vara tydligt fastställt. Ansvaret för en del av de faktorer som beskrivs eller krävs kan genom olika avtals- och upphandlingsarrangemang (till exempel upphandling av tjänster, applikationsuthyrning, användande av underleverantörer) vila på någon annan än objektet för egenkontroll av informationssäkerheten.

Om ansvaret som ingår i informationssäkerhetsplanen vilar på någon annan än objektet för egenkontroll av informationssäkerheten, ska ansvaret fastställas i uppdragsavtal eller andra avtal mellan parterna. Även producenter av köpta tjänster, eventuella producenter av utkontrakterade tjänster och andra eventuella avtalsparter ska omfattas av tydliga ansvar för informationssäkerhet och behandling av kunduppgifter. Av avtalen ska det också framgå vilka åtgärder parterna ska vidta gemensamt eller var för sig om det förekommer brister, problem eller faktiska risker i informationssäkerheten.

Innehållet i informationssäkerhetsplanen bör utformas med hänsyn till omfattningen av den verksamhet som objektet för egenkontroll beskriver samt med hänsyn till de ändamålsenliga informationssäkerhets- och dataskyddsrutiner som behövs i organisationens verksamhetsmiljö. De eventuella risker som verksamheten medför samt de resurser som står till förfogande för att upprätthålla och säkra verksamheten (interna eller via utkontraktering) ska bedömas, avtalas och ordnas på förhand, så att man i alla slags situationer har möjlighet att reagera snabbt vid behov och följaktligen korrekt inrikta relevanta säkerhetsåtgärder för kunduppgifter.

Oberoende av storleken på den organisation som är objekt för egenkontroll av informationssäkerheten ska den ha ändamålsenliga rutiner för att skydda känsliga kunduppgifter i digitala och icke-digitala miljöer. Dessa egna rutiner som objektet för egenkontroll av informationssäkerheten har infört ska också följas när klient- eller patientuppgifter behandlas i den berörda organisationen.

Objektet för egenkontroll av informationssäkerheten ska ha ett avtal om behandlingen av kunduppgifter och säkerställandet av informationssäkerheten som gäller de inbördes ansvarsförhållandena mellan andra tjänstetillhandahållare som använder tjänstetillhandahållarens klient- eller patientdatasystem. Objektet för egenkontroll av informationssäkerheten ansvarar för informationssäkerhetsplanen också i situationer där den till exempel köper en driftmiljö eller it-tjänster från andra tjänstetillhandahållare eller producenter av informationssystemtjänster enligt lagen om kunduppgifter eller andra producenter av informationssystemtjänster.

Genom ömsesidiga avtal kan man dock inte fastställa eller avtala om ansvar på ett sätt som avviker från vad som bestäms i lagen om kunduppgifter.

Utifrån informationssäkerhetsplanens faktiska innehåll eller innehållet som presenteras i de bilagor som det hänvisas till i planen ska man vid behov kunna verifiera följande aspekter som gäller egenkontrollen av informationssäkerheten:

- att en informationssäkerhetsplan har utarbetats,
- att informationssäkerhetsplanen innehåller den information som krävs enligt denna föreskrift,
- att informationssäkerhetsplanen beskriver hur planen uppdateras och granskas regelbundet och
- hur genomförandet av planen följs upp.

Objektet för egenkontroll av informationssäkerheten ska kunna påvisa att det finns en informationssäkerhetsplan, att den är ändamålsenlig och hur den genomförs till exempel för tillsynsmyndigheterna, även i situationer där det inte själv producerar tjänsterna. Detta gäller både vid produktion av social- och hälsovårdstjänster och vid produktion av informationssystemtjänster eller tekniska stödtjänster. Även då ska man beskriva och vid behov kunna verifiera vem som bär ansvaret för att saken beskrivs eller utförs och hur man har försäkrat sig om att saken har beskrivits eller utförts på erforderligt sätt.

4 Förhållande till THL:s övriga föreskrifter, allmänna referensramar och vissa andra författningar

Utöver denna föreskrift 3/2024 från THL ska man vid utarbetandet av en informationssäkerhetsplan tillämpa THL:s föreskrift 5/2024 (se särskilt kapitel 9) om väsentliga krav på funktionalitet och informationssäkerhetskrav hos informationssystem för social- och hälsovården med inriktning på de informationssystem som är avsedda för behandling av kunduppgifter. Tjänstetillhandahållare och apotek ska använda informationssystem vars användningsändamål svarar mot tjänstetillhandahållarens och apotekets egen verksamhet. Dessutom ska tjänstetillhandahållaren och apoteket uppfylla de väsentliga krav som gäller verksamheten (84 § i lagen om kunduppgifter). De väsentliga kraven kan uppfyllas med en helhet som består av ett eller flera informationssystem. I bilaga 1 till THL:s föreskrift 4/2024 om klassificering och certifiering av informationssystem för social- och hälsovården beskrivs klassificeringen av informationssystem med praktiska exempel. När informationssäkerhetsplanen granskas och underhålls ska även andra gällande bestämmelser om informationssäkerhet följas.

Vid utarbetandet av informationssäkerhetsplanen rekommenderas standarder och referensramar avsedda för planering av informationssäkerheten, till exempel standarderna i ISO/IEC 27000-serien eller referensramen för arkitekturen för digital säkerhet som publicerats av Myndigheten för digitalisering och befolkningsdata.

I denna föreskrift föreskrivs inte om vilka störningar i informationssystemens driftmiljöer och operativa nätmiljöer som är betydande eller hur anmälningar om störningar ska göras (90 § i lagen om kunduppgifter). Hanteringen av avvikelser i anslutning till informationsnät och driftmiljöer inom social- och hälsovården kommer potentiellt att regleras med stöd av NIS 2-bestämmelserna i en lag om hantering av cybersäkerhetsrisker som är under beredning[2].

Tillämpningsområdet för denna föreskrift är inte användningsändamål enligt lagen om sekundär användning av social- och hälsovårdsuppgifter (552/2019, lagen om sekundär användning). Tjänstetillhandahållaren kan dock i sin informationssäkerhetsplan även beakta kraven på behandlingen av uppgifter i lagen om sekundär användning. Vissa informationssystem kan ha användningsändamål enligt både lagen om kunduppgifter och lagen om sekundär användning.

---

[2] Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148.

NIS2-direktivet kommer att införlivas i den nationella lagstiftningen senast den 17 oktober 2024, och genomförandebestämmelserna kommer att börja tillämpas från och med den 18 oktober 2024. I regeringens proposition till riksdagen om genomförande av cybersäkerhetsdirektivet föreslås att det stiftas en ny lag om hantering av cybersäkerhetsrisker. I lagförslaget föreslås bestämmelser om riskhantering i anslutning till informationsnät och driftmiljöer.

Tillämpningsområdet för denna föreskrift är inte bestämmelserna om medicintekniska produkter (jfr kapitel 6.2 Förfaranden vid fel och problem samt kontinuitetshantering vs. tjänstetillhandahållarens anmälningsskyldigheter).

Lagen om informationshantering inom den offentliga förvaltningen (906/2019, informationshanteringslagen) är en allmän lag som tillämpas på informationshantering och användning av informationssystem då myndigheter behandlar informationsmaterial. I 13 § i informationshanteringslagen föreskrivs om informationshanteringsenheters skyldighet att säkerställa informationssäkerheten i sin verksamhet. Den informationssäkerhetsplan som avses i 77 § i lagen om kunduppgifter är obligatorisk för alla tjänstetillhandahållare inom social- och hälsovården; genom informationssäkerhetsplanen säkerställs enhetliga förfaranden vid behandling av kunduppgifter både för offentliga och privata tjänstetillhandahållare, mellanhänder och Folkpensionsanstalten. I synnerhet kapitel 2 (Ordnande av informationshantering) och 4 (Informationssäkerhet) i informationshanteringslagen innehåller punkter som är förpliktande för myndigheterna och informativa för privata aktörer och som måste eller med fördel bör tillämpas i informationssäkerhetsplanen för objektet för egenkontroll av informationssäkerheten.

5 Allmänt om informationssäkerhetsplanen

Informationssäkerhetsplanen är ett praktiskt verktyg för att ge en helhetsbild av informationssäkerheten och genomföra behandlingen av kunduppgifter enligt god praxis. De redogörelser och rutiner som beskrivs i informationssäkerhetsplanen kan kombineras med övriga anvisningar, kvalitetshandböcker eller informationssäkerhetspolicyer som styr dataskyddet och informationssäkerheten hos objektet för egenkontroll av informationssäkerheten. Beskrivningarna kan vid behov vara informationssystemspecifika eller gemensamma för flera aktörer som omfattas av samma plan. Alla beskrivningar behöver inte ingå i informationssäkerhetsplanen, utan planen kan hänvisa till beskrivningar som finns tillgängliga separat, till exempel informationssäkerhetsanvisningarna hos objektet för egenkontroll av informationssäkerheten eller beskrivningar av informationssystemportföljen.

En informationssäkerhetsplan enligt denna föreskrift ska inte inkluderas i eller kombineras med planer för egenkontroll som publiceras eller som är offentligt tillgängliga. Informationssäkerhetsplanen och de bilagor som den hänvisar till ska hanteras och förvaras på ett datasäkert sätt. De ska skyddas mot åtkomst av utomstående och vid behov ska informationen i dem märkas som sekretessbelagd. En tjänstetillhandahållare som fungerar som myndighet ska beakta bestämmelserna om sekretess i lagen om offentlighet i myndigheternas verksamhet (621/1999, offentlighetslagen) (24 § 1 mom. 7 punkten).

Syftet med informationssäkerhetsplanen är att säkerställa att de som behandlar kunduppgifter och som använder och producerar uppgifterna förstår ansvaret i anslutning till behandlingen av kunduppgifter och i varje enskilt tillfälle kan agera så att kunduppgifternas integritet, konfidentialitet, tillgänglighet, oavvislighet och autenticitet förverkligas.

Syftet med informationssäkerhetsplanen är att säkerställa att man vid behandlingen av kunduppgifter på ett riskbaserat och heltäckande sätt beaktar faktorer som rör dataskydd och informationssäkerhet i verksamheten hos objektet för egenkontroll av informationssäkerheten och i informationssystemens driftmiljö. Med hjälp av de förfaranden och metoder som beskrivs i informationssäkerhetsplanen kan man som en del av riskhanteringen förebygga att risker förverkligas. Informationssäkerhetsplanen ska utarbetas utifrån en bedömning av eventuella risker, de sannolikheter som är förknippade med dem och konsekvenserna av de identifierade riskerna. Dessutom ska man i informationssäkerhetsplanen bedöma följderna av att riskerna minskas (acceptabla kvarvarande risker) eller undanröjs helt.

Med de förfaranden och metoder som beskrivs i informationssäkerhetsplanen säkerställs dessutom att andra informationssystem eller applikationer som är anslutna till informationssystemen, och som inte är avsedda för behandling av klient- och patientuppgifter, inte äventyrar informationssystemens prestanda eller egenskaper när det gäller informationssäkerhet och dataskydd.

När det gäller användningen av FPA:s riksomfattande informationssystemtjänster ska informationssäkerhetsplanen också redogöra för frågor som gäller dataskydd och informationssäkerhet. Tjänstetillhandahållare och apotek ska i informationssäkerhetsplanen redogöra för hur kraven på informationssäker användning och dataskydd har säkerställts och hur rutinerna för dataskydd och informationssäkerhet har ordnats innan de ansluter sig som användare av Kanta-tjänsterna (se kapitel 6.12 Informationssäkerhetsrutiner för anslutning till Kanta-tjänsterna och användning av dem).

Informationssäkerhetsplanen är ett dokument utarbetat av objektet för egenkontroll av informationssäkerheten, med vilket den personuppgiftsansvarige kan komplettera sin ansvarsskyldighet enligt EU:s allmänna dataskyddsförordning (artikel 5.2) [3] . Den personuppgiftsansvarige, dvs. objektet för egenkontroll av informationssäkerheten, kan fullgöra sin ansvarsskyldighet till exempel genom att dokumentera utförda åtgärder och utarbeta en konsekvensbedömning, ett databokslut och ett register över behandling. Ansvarsskyldigheten kan också fullgöras genom andra motsvarande förfaranden som påvisar att den personuppgiftsansvariges och personuppgiftsbiträdets verksamhet följer bestämmelserna.

De faktorer som beskrivs i informationssäkerhetsplanen ska vid behov kunna verifieras hos den tillsynsmyndighet som granskat att egenkontrollen av informationssäkerheten är genomförd.

6 Redogörelser och krav som ska tas in i informationssäkerhetsplanen

Enligt 77 § 1 mom. punkterna 1–9 och 77 § 2 mom. i lagen om kunduppgifter ska informationssäkerhetsplanen innehålla redogörelser för hur kraven på behandlingen av kunduppgifter och på informationssystemen säkerställs.

I informationssäkerhetsplanen ska underpunkterna 6.1–6.12 i kapitel 6 i denna föreskrift beskrivas i samband med den egna verksamheten och de informationssäkerhetslösningar som används hos objektet för egenkontroll av informationssäkerheten.

Utöver kraven i 77 § i lagen om kunduppgifter kan informationssäkerhetsplanen också omfatta andra omständigheter som är väsentliga för objektet för egenkontroll av informationssäkerheten.

Enligt 78 § i lagen om kunduppgifter ska den ansvariga föreståndaren hos en tjänstetillhandahållare inom social- och hälsovården och apotekaren se till att en informationssäkerhetsplan enligt 77 § utarbetas, regelbundet uppdateras och iakttas. Som en del av planen ska man beskriva hur planen genomförs och hur egenkontrollen av informationssäkerheten ordnas i praktiken.

Informationssäkerhetsplanen kan hänvisa till befintliga anvisningar och bilagedokument som ska upprätthållas separat (jfr kapitel 5). Det väsentliga är att det av planen framgår var man kan hitta dokumentationen eller hur man kan verifiera att kraven uppfylls. De helheter och tillvägagångssätt som krävs kan beskrivas direkt i informationssäkerhetsplanen om det inte finns eller går att få tag på annan färdig dokumentation[4].

[3] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (EU:s allmänna dataskyddsförordning)

[4] Obs! Formuleringarna i detta kapitel 6 såsom ”i informationssäkerhetsplanen ska ... beskrivas” eller andra motsvarande krav på beskrivning som enbart hänvisar till informationssäkerhetsplanen kan alltid också tolkas som ”i informationssäkerhetsplanen eller i de bilagor som den hänvisar till ska ...beskrivas”.

6.1 Allmänna informationssäkerhetsrutiner

Enligt 77 § 1 mom. 5 punkten i lagen om kunduppgifter ska informationssystemens driftmiljö vara lämplig för en sådan ändamålsenlig användning av informationssystemen som säkerställer informationssäkerheten och dataskyddet. Hanteringen av risker i driftmiljön och informationssystemen ska ombesörjas. Ett rekommenderat exempel på god praxis, i synnerhet för stora organisationer, är ett system för hantering av informationssäkerheten som överensstämmer med standarderna i ISO/IEC 27000-serien. För mindre tjänstetillhandahållare rekommenderas till exempel en självutvärdering med hjälp av Cybersäkerhetsmätaren[5], som tillhandahålls av Cybersäkerhetscentret vid Traficom.

Informationssäkerhetsplanen ska innehålla en beskrivning av de allmänna informationssäkerhetsrutinerna och/eller gällande policyer som rör digital säkerhet, om sådana upprättats, hos objektet för egenkontroll av informationssäkerheten [6] . Dessutom ska planen innehålla uppgifter om register över behandlingen av personuppgifter, avtal om behandlingen av kunduppgifter, centrala informationssäkerhetsanvisningar och dataskyddsombud. Av informationssäkerhetsplanen ska det också framgå hur dokumentationen regelbundet ses över och utvecklas samt hur ansvaret i informationssäkerhetsarbetet har fördelats och organiserats för att man ska uppnå verksamhetsmålen och hantera riskerna i verksamheten.

Enligt 78 § 4 mom. i lagen om kunduppgifter finns bestämmelser om utnämning av ett dataskyddsombud och om dataskyddsombudets ställning och uppgifter i artiklarna 37–39 i EU:s allmänna dataskyddsförordning. Objektet för egenkontroll av informationssäkerheten ska således utse ett eller flera dataskyddsombud i enlighet med ovan nämnda bestämmelser. Dataskyddsombudet ska ha en tydlig och dokumenterad uppgiftsbeskrivning där skyldigheterna i anslutning till behandlingen av kunduppgifter beaktas. Dataskyddsombudet ska ha en för uppgiften lämplig kompetens och resurser att sköta uppgiften för objektet för egenkontroll av informationssäkerheten med beaktande av ansvaret och skyldigheterna gällande registerföring och behandling av personuppgifter, organisationens storlek och verksamhetens omfattning.

I informationssäkerhetsplanen eller de bilagor som den hänvisar till ska man beskriva riktlinjerna för distans- och hybridarbete för personal som arbetar på distans (till exempel hemma eller på en annan distansarbetsplats) och i olika mobila patient- och klientarbeten, om det i verksamheten hos objektet för egenkontroll av informationssäkerheten förekommer användning av kunduppgifter på distans.

Informationssäkerhetsplanen ska beskriva det innehåll i kunduppgifterna som anställda i olika arbetsuppgifter behöver. Till exempel bör de kunduppgifter som informationsförvaltningsexperter och personal inom utvecklings- och upphandlingsverksamhet eventuellt använder i sitt arbete motsvara den information som är nödvändig i just deras arbetsuppgifter (jfr kapitel 6.7).

[5] https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren

[6] Policyer som rör digital säkerhet är till exempel informationssäkerhets- och dataskyddspolicyer.

6.2 Förfaranden vid fel och problem samt kontinuitetshantering

Objektet för egenkontroll av informationssäkerheten ska förbereda sig på fel och problem, informationssäkerhetsincidenter[7], kränkningar av informationssäkerheten och andra störningar så att kontinuiteten i behandlingen av kunduppgifter kan hanteras och tryggas under olika förhållanden. Objektet för egenkontroll av informationssäkerheten ska i händelse av fel och problem ha på förhand fastställda och tydliga tillvägagångssätt, anvisningar och ansvar för att observera, informera om, åtgärda och återhämta sig från sådana situationer och informationssäkerhetsincidenter. På motsvarande sätt föreskrivs i 13 a § i informationshanteringslagen att en informationshanteringsenhet ska följa upp informationssäkerhetens tillstånd i sin verksamhetsmiljö och säkerställa informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel. Dessutom ska informationshanteringsenheten identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen.

De informationssystem som används ska klassificeras utifrån hur kritiska de är. Klassificeringen av kritiskhet ska göras med tanke på den egna verksamheten och riskerna och målen i anslutning till den. Klassificeringen kan påverka beredskapsrutinerna. Dessa faktorer ska beskrivas direkt i informationssäkerhetsplanen eller i de separata kontinuitets-, återhämtnings- och beredskapsplanerna som informationssäkerhetsplanen hänvisar till och som innehåller de förfaranden som ska iakttas av objektet för egenkontroll av informationssäkerheten vid fel och problem.

Objektet för egenkontroll av informationssäkerheten ska definiera hur kritiska de viktigaste informationssystemen och deras komponenter är med tanke på patient- och klientsäkerheten. Det väsentliga är att identifiera kritiska informationssystem och delsystem, enheter och andra resurser som är kritiska för informationssystemens funktion. Systemens tillförlitlighet måste garanteras till exempel genom fungerande dupliceringar, planerade tillfälliga lösningar, reservdelar, specialkomponenter och aktiva övervaknings- och underhållsåtgärder.

Objektet för egenkontroll av informationssäkerheten ska planera de åtgärder som krävs för att återhämta sig från störningar i informationssystemen samt anvisningar och upphandlingar i samband med dessa. De tillvägagångssätt som planerats med tanke på situationer som avviker från det normala och exceptionella förhållanden ska regelbundet gås igenom, testas och ses över så att tillgången till nödvändiga anvisningar är tryggad i praktiken i särskilda situationer. Man bör öva på de planerade rutinerna till exempel en gång per år.

Beskrivningarna av utredningspraxis och hanteringsmodeller samt fastställandet av ansvar ska göras med tanke på nätverks- och datakommunikationsproblem, problem med användningen av informationssystem samt observerade och faktiska kränkningar av informationssäkerheten. Dessutom ska man beskriva hur objektet för egenkontroll av informationssäkerheten kan få tillgång till detaljerad uppföljningsinformation om en störningssituation, till exempel händelseloggar med tidsstämplar, för att utreda situationen och det som inträffat.

Dessutom är det viktigt att planera underhåll, uppdateringar och vid behov förnyelser av informationssystem, enheter och nätverk. På så sätt säkerställer man att nödvändiga komponent- och programuppdateringar sköts i god tid innan eventuella fel inträffar. Hur kritiska komponenterna är ska granskas särskilt med tanke på klient- och patientsäkerheten.

---

[7] Ordlista om cybersäkerhet, Säkerhetskommittén 2018: *informationssäkerhetsincident*: en eller flera sammanhängande oväntade eller oönskade informationssäkerhetshändelser som äventyrar informationssäkerheten för uppgifter och tjänster och påverkar organisationens verksamhet på ett ofördelaktigt sätt (ursprunglig definition på finska, egen översättning).

Det rekommenderas att alla relevanta uppgifter om händelser som hotar säkerheten ska samlas in med tanke på en eventuell utredning av en säkerhetsincident. Dessutom rekommenderas det att man utreder den/de bakomliggande orsakerna till informationssäkerhetsincidenten för att kunna upptäcka eventuella sårbarheter som äventyrar informationssäkerheten och utreda om incidenten var avsiktlig eller oavsiktlig, orsakad av en extern eller intern aktör osv.

Det rekommenderas att objekt för egenkontroll av informationssäkerheten implementerar en eller flera rapporteringskanaler via vilka en person inom eller utanför organisationen kan rapportera misstänkta informationssäkerhetsincidenter.

Tjänstetillhandahållare och apotek ska underrätta producenten av en informationssystemtjänst om betydande avvikelser från de väsentliga kraven på ett informationssystem och en välbefinnandeapplikation (90 § 1 mom. i lagen om kunduppgifter). Betydande avvikelser från kraven beskrivs i kapitel 10.4 i THL:s föreskrift 5/2024.

Objektet för egenkontroll av informationssäkerheten ska underrätta Valvira om betydande avvikelser i ett informationssystem eller en välbefinnandeapplikation när det gäller uppfyllandet av de väsentliga kraven, i synnerhet i situationer där en sådan avvikelse kan medföra en betydande risk för klient- eller patientsäkerheten eller informationssäkerheten (90 § 1 mom. i lagen om kunduppgifter). Även andra aktörer kan anmäla risker som de observerat till Valvira. Korrigerande åtgärder ska vidtas utan dröjsmål för att åtgärda betydande avvikelser.

Den personuppgiftsansvarige ska underrätta dataombudsmannen om observerade personuppgiftsincidenter. Bestämmelser on anmälan av personuppgiftsincidenter finns i artikel 33 i EU:s allmänna dataskyddsförordning (90 § 1 mom. i lagen om kunduppgifter). Hanteringen av personuppgiftsincidenter ska vara dokumenterad antingen direkt i informationssäkerhetsplanen eller i andra dokument hos objektet för egenkontroll av informationssäkerheten.

En tjänstetillhandahållare, ett apotek, FPA och en producent av en informationssystemtjänst eller en tillverkare av ett informationssystem eller en mellanhand ska utan dröjsmål underrätta Valvira om sådana betydande störningar i anslutning till informationssäkerheten i de driftmiljöer och informationsnät som aktören använder och till följd av vilka användningen av informationssystem och tillhandahållandet av social- och hälsovårdstjänster kan äventyras avsevärt (90 § 2 mom. i lagen om kunduppgifter).

Om ett informationssystem eller en välbefinnandeapplikation uppfyller definitionen av en medicinteknisk produkt, ska tjänstetillhandahållaren i enlighet med 33 § i lagen om medicintekniska produkter (719/2021) underrätta Fimea om sådana tillbud i anslutning till medicintekniska produkter som avses i bestämmelsen, till exempel en avvikelse eller störning i prestanda hos ett informationssystem som räknas som en medicinteknisk produkt.

6.3 Personalens utbildning samt upprätthållande och utveckling av kompetensen

Med hjälp av informationssäkerhetsplanen säkerställs att personalen vid objektet för egenkontroll av informationssäkerheten behärskar informationssystemen som de använder och beaktar kraven på sekretess och informationssäkerhet i fråga om kunduppgifter samt förstår följderna av missbruk.

Informationssäkerhetsplanen ska beskriva hur utbildning har ordnas för de personer som använder informationssystemen, dvs. hur man i praktiken säkerställer den utbildning och kompetens som användningen av systemen kräver. De personer som använder informationssystemen ska ha utbildning både i behandling av kunduppgifter och i dataskydds- och informationssäkerhetsfrågor.

Utbildningen som erbjuds personalen bör till omfattningen och innehållet vara tillräcklig och ändamålsenlig med tanke på personens eller personalgruppens arbets- och databehandlingsuppgifter. Utbildning bör erbjudas regelbundet både för att upprätthålla befintliga färdigheter, för att sköta nya uppgifter eller situationer och för nya

arbetstagare. På motsvarande sätt föreskrivs i 4 § 2 mom. 3 punkten i informationshanteringslagen att en informationshanteringsenhets ledning ska ombesörja att det vid enheten kan erbjudas utbildning varmed det säkerställs att de anställda och personer som arbetar för informationshanteringsenhetens räkning är tillräckligt förtrogna med gällande författningar, föreskrifter och med informationshanteringsenhetens anvisningar om informationshantering och databehandling samt om offentlighet och sekretess i fråga om handlingar.

Objektet för egenkontroll av informationssäkerheten ska ha en utbildningsplan eller motsvarande dokument som beskriver verksamhetsmodellen för inskolning och utbildning av personalen samt för upprätthållande, uppföljning och uppdatering av personalens kompetens inom behandling av kunduppgifter samt dataskydds- och informationssäkerhetsfrågor. Utbildningsplanen ska beskriva innehållet i den utbildning som krävs i olika arbetsuppgifter och roller och hur utbildningen genomförs. Den utbildning och kompetens som krävs av dem som använder informationssystemet kan verifieras med intyg, anteckningar om deltagande i utbildningar eller på något annat sätt som man kommit överens om i organisationen.

Informationssäkerhetsplanen ska beskriva hur personalen utbildas i och informeras om grunderna för behandling av kunduppgifter. Dessa är till exempel betydelsen av att dokumentera kunduppgifter, betydelsen av att använda och skydda kunduppgifter, ansvaret för den som behandlar uppgifterna samt förekomsten av och betydelsen av egenkontroll av informationssäkerheten och myndighetstillsyn i anslutning till behandlingen av uppgifterna.

Bestämmelser om grunderna för utlämnande av uppgifter finns i flera lagar. När uppgifter lämnas ut ska de personer som lämnar ut kunduppgifter kontrollera den lagliga grund på vilken kunduppgifterna kan lämnas ut till mottagaren. Dessutom ska personer som lämnar ut kunduppgifter se till att mottagaren får kunduppgifter endast till den del som mottagaren har rätt till enligt lag. Praktiska kunskaper i anslutning dessa frågor bör ingå i utbildningen och introduktionen av personalen. Personer som lämnar ut kunduppgifter ska i de informationssystem som används också säkerställa att det skapas ett meddelande om utlämnande eller en utlämningslogg när uppgifter lämnas ut.

6.4 Informationssystemens bruksanvisningar och användning av systemen enligt anvisningarna

De egna anvisningarna och tillvägagångssätten hos objektet för egenkontroll av informationssäkerheten ska styra dem som behandlar kunduppgifter i sina arbetsuppgifter och roller till rätt tillvägagångssätt och korrekt behandling av kunduppgifter.

Informationssäkerhetsplanen ska beskriva hur man säkerställer en ändamålsenlig och informationssäker användning av informationssystemet i verksamheten och driftmiljön hos objektet för egenkontroll av informationssäkerheten i enlighet med anvisningarna från producenten av en informationssystemtjänst och/eller tillverkaren av informationssystemet. På motsvarande sätt föreskrivs i 4 § 2 mom. 2 punkten i informationshanteringslagen att informationshanteringsenhets ledning ska ombesörja att det vid enheten finns uppdaterade anvisningar om hantering av informationsmaterial, om användning av informationssystem, om databehandlingsrättigheter, om informationshanteringsansvar, om informationsrättigheter, om informationssäkerhetsåtgärder samt om beredskap för undantagsförhållanden.

Informationssäkerhetsplanen ska beskriva hur man säkerställer de som använder informationssystemen har tillgång till nödvändiga och aktuella anvisningar från organisationen (verksamhetsmodeller) och bruksanvisningar för informationssystemen. Dessa anvisningar ska finnas åtminstone på det språk i vilket kunskaper är ett minimikrav för att kunna sköta arbetsuppgiften i fråga. Anvisningarna ska vara lättillgängliga för personalen och alla ska känna till var de finns.

Alla anställda som behandlar kunduppgifter ska ges skriftliga anvisningar om behandlingen av kunduppgifter. Bruksanvisningarna och övriga nödvändiga anvisningar ska vara begripliga och motsvara de versioner av informationssystemen som används i organisationen. I anvisningarna bör man sträva efter entydighet och beakta olika arbetsuppgifter och roller.

Det ska framgå av informationssäkerhetsplanen i vilka distributionskanaler man kan hitta anvisningarna och utbildningsmaterialet från producenten av en informationssystemtjänst. Planen ska beskriva organisationens egna tillvägagångssätt för att följa upp att anvisningarna från producenten av en informationssystemtjänst iakttas. Dessutom ska informationssäkerhetsplanen innehålla en beskrivning av hur uppdatering och distribution av bruksanvisningarna genomförs i praktiken i samband med versionsuppdateringar och andra ändringar av informationssystem, andra informationssystem och programvara.

6.5 Informationssystemens basuppgifter, beskrivningar och uppfyllande av väsentliga krav

Objektet för egenkontroll av informationssäkerheten ska i sin informationssäkerhetsplan beskriva de basuppgifter och närmare beskrivningar av alla informationssystem och välbefinnandeapplikationer[8] som de använder och som avses i lagen om kunduppgifter och som är avsedda för:

- elektronisk behandling av kunduppgifter
- registrering och uppdatering av kundhandlingar
- anslutning till de riksomfattande informationssystemtjänsterna
- välbefinnandeapplikationer eller digitala ärendetjänster som används i tjänstetillhandahållarens verksamhet eller
- utnyttjande av uppgifter om välbefinnande i arbetet som utförs av yrkesutbildade personer inom social- och hälsovården.

Objektet för egenkontroll av informationssäkerheten ska i informationssäkerhetsplanen beskriva var information finns om klassificerade och oklassificerade informationssystem som används i verksamheten hos objektet för egenkontroll av informationssäkerheten (jfr THL:s föreskrift 4/2024):

- certifierade – informationssäkerhetsbedömda och samtestade informationssystem i klass A2 eller A3 som ska anslutas till Kanta-tjänsterna och som är avsedda för behandling av klientuppgifter inom socialvården eller patientuppgifter
- certifierade – informationssäkerhetsbedömda informationssystem i klass A1 som är avsedda för behandling av klientuppgifter inom socialvården eller patientuppgifter
- informationssystem i klass B avsedda för behandling av klientuppgifter inom socialvården eller patientuppgifter samt

[8] Förutom beskrivningar av informationssystemen ska informationssäkerhetsplanen också innehålla beskrivningar av välbefinnandeapplikationer och andra digitala ärendetjänster som riktas till kunder och som används i verksamheten hos objektet för egenkontroll av informationssäkerheten. I THL:s föreskrift 4/2024, kapitel 2 Definitioner, definieras välbefinnandeapplikationer och digitala ärendetjänster som tillsammans bildar en digital tjänst.

Digital tjänst: den allmänna termen digital tjänst används i föreskrifterna 4/2024 och 5/2024 med hänvisning till både välbefinnandeapplikationer och digitala ärendetjänster. Termen omfattar både informationssystem och välbefinnandeapplikationer med egenskaper som är avsedda att vara direkt tillgängliga för medborgarna. Till de digitala tjänsterna kan räknas både digitala ärendetjänster och sådana välbefinnandeapplikationer som är anslutna till Kanta-tjänster såsom datalagret för egna uppgifter. Det är också möjligt att en digital tjänst uppfyller definitionen av både välbefinnandeapplikation och informationssystem i lagen om kunduppgifter.

- andra informationssystem (oklassificerade) som inverkar och som ska beaktas vid installationer, drift och uppdateringar enligt informationssäkerhetsplanen med tanke på skyddet av känsliga kunduppgifter.

Informationssäkerhetsplanen ska beskriva åtminstone följande aspekter av de informationssystem och välbefinnandeapplikationer som används:

- basuppgifter: namn, version (eller motsvarande statusuppgift), leverantör, kontaktuppgifter, uppgifter om FPA:s samtestning (klasserna A2 och A3), uppgifter om intyget över bedömning av informationssäkerheten (klasserna A1, A2 och A3) och dess överensstämmelse med uppgifterna i Valviras register över informationssystem (klasserna B, A1, A2 och A3) samt även uppgifter om digitala ärendetjänster i anslutning till den egna verksamheten,
- informationssystemets eller välbefinnandeapplikationens användningsändamål,
- användargrupper samt
- de rutiner och förfaranden, specifika för informationssystemet och välbefinnandeapplikationen, som beskrivs i denna föreskrift.

Informationssäkerhetsplanen ska omfatta alla informationssystem och välbefinnandeapplikationer som används av objektet för egenkontroll av informationssäkerheten. Informationssäkerhetsplanen ska också innehålla uppgifter om sådana digitala ärendetjänster (informationssystem) som är knutna till den egna verksamheten.

En tjänstetillhandahållare och ett apotek ska i enlighet med 77 § 1 mom. 8 punkten i lagen om kunduppgifter säkerställa att de informationssystem som avses i 79 § uppfyller de väsentliga kraven för sitt användningsändamål i enlighet med 84 § 2 mom. Tjänstetillhandahållare och apotek ska använda informationssystem [9] vars användningsändamål svarar mot tjänstetillhandahållarens och apotekets egen verksamhet. Informationssystemen måste uppfylla väsentliga krav på funktionalitet.

Tjänstetillhandahållare och apotek ansvarar för att de väsentliga kraven uppfylls i deras egen verksamhet. De väsentliga kraven kan uppfyllas med en helhet som består av ett eller flera informationssystem. Förfarandena för att säkerställa kraven ska beskrivas i informationssäkerhetsplanen.

I enlighet med föreskrift 5/2024 ska tjänstetillhandahållare och apotek beakta väsentliga krav i sin egen verksamhet när informationssystem tas i bruk och används för produktion av tjänster samt i verksamheten enligt informationssäkerhetsplanen. Dessutom ska det säkerställas att de väsentliga kraven på informationssystem och välbefinnandeapplikationer uppfylls i samband med upphandling, utveckling och upprätthållande av informationssystem samt i samband med avtal som rör informationssystemen. Tjänstetillhandahållare och apotek kan använda uppgifterna i Valviras register över informationssystem för att säkerställa att de väsentliga kraven uppfylls.

[9] Producenten av en informationssystemtjänst, tillverkaren av ett informationssystem och tillverkaren av en välbefinnandeapplikation ska uppfylla de väsentliga kraven på informationssystem som används i tjänstetillhandahållarens och apotekets verksamhet (jfr

Valvira för ett offentligt register över informationssystem avsedda för behandling av kunduppgifter (80 § 2 mom. i lagen om kunduppgifter). Uppgifterna i Valviras register över informationssystem grundar sig på anmälningar från producenter av informationssystemtjänster och resultaten av certifieringen av system i klass A. Valviras register över informationssystem innehåller uppgifter om vilka väsentliga krav som har uppfyllts i olika informationssystem och hur uppfyllandet av de väsentliga kraven har verifierats i system som hör till klass A. Innehållet i informationssäkerhetsplanen för informationssystemen bör nyttja den information som finns i Valviras register över informationssystem om vilka minimikravprofiler enligt THL:s föreskrift 5/2024 som de informationssystem som används i den egna verksamheten uppfyller.

Objektet för egenkontroll av informationssäkerheten ska beakta och följa eventuella preciseringar som publiceras i Valviras register över informationssystem för att se till att informationssystemen och välbefinnandeapplikationerna uppfyller kraven. Samtidigt bör man identifiera vilka användningsändamål i enlighet med profilerna som ska implementeras i de informationssystem som används i den egna verksamheten.

Objektet för egenkontroll av informationssäkerheten ska i sin informationssäkerhetsplan beskriva hur man säkerställer att informationssystemens prestanda och deras egenskaper när det gäller informationssäkerhet eller dataskydd inte äventyras. Beskrivningen gäller informationssystem som ansluts till Kanta-tjänsterna eller andra applikationer eller andra informationssystem som används i deras driftmiljö, vilket avser till exempel datorprogram som inte behandlar kunduppgifter och således inte är informationssystem i klass A eller B enligt 79 § i lagen om kunduppgifter.

Informationssäkerhetsplanen kan också täcka sådana applikationsprogram eller informationssystem som används vid objektet för egenkontroll av informationssäkerheten, men som inte behandlar kunduppgifter.

6.6 Installation, drift och uppdatering av informationssystem

Enligt 81 § 2 mom. i lagen om kunduppgifter får ett informationssystem eller en välbefinnandeapplikation som är avsett för behandling av kunduppgifter inte tas i användning för produktion av tjänster, om det inte finns giltiga uppgifter om det i Valviras register över informationssystem, eller om intyget över bedömning av informationssäkerhet för ett informationssystem eller en välbefinnandeapplikation som hör till klass A har gått ut Detta beskrivs i detalj i THL:s föreskrift 4/2024, kapitel 9 Förutsättningar för ibruktagande av Informationssystemet eller välbefinnandeapplikationen.

I informationssäkerhetsplanen ska man beskriva tillvägagångssätten för installation, drift och uppdatering av informationssystem hos objektet för egenkontroll av informationssäkerheten samt säkerställande av informationssäkerheten i anslutning till dessa. Beskrivningarna ska också ange personalens roller vid installation, drift och uppdatering. Förfaranden för ändringshantering, testning och godkännande samt ansvarsfördelningen i installations-, drift- och uppdateringsarbetet ska inkluderas i planen. Beskrivningen ska göras på en sådan precisionsnivå som bäst stöder och styr riskhanteringen i anslutning till informationssäkerheten och behandlingen av kunduppgifter. Samtidigt ska man överväga brådskande installation av uppdateringar i anslutning till sårbarheter som eventuellt utnyttjas i stor utsträckning samt andra reparations- och skadebegränsningsåtgärder som kan avvika från de testnings- och godkännandeförfaranden för informationssystem som används i normala situationer.

Informationssäkerhetsplanen ska beskriva installation, underhåll och uppdatering av informationssystemen i enlighet med anvisningarna från producenten av en informationssystemtjänst. Avtal som ingås med producenter av en informationssystemtjänst ska beskriva de frågor som är väsentliga med tanke på driftmiljön hos objektet för egenkontroll av informationssäkerheten.

Det ska framgå av informationssäkerhetsplanen vilken yrkesskicklighet och sakkunskap som krävs av personalen som installerar, driver och uppdaterar informationssystemen. Även dessa personers roller och ansvar ska fastställas i förhållande till objektet för egenkontroll av informationssäkerheten samt producenten av en informationssystemtjänst.

I 77 § 1 mom. 7 punkten i lagen om kunduppgifter föreskrivs att informationssystemen endast ska installeras, drivas och uppdateras av personer med den yrkesskicklighet och sakkunskap som behövs för det och vars tillförlitlighet har säkerställts på det sätt som avses i 12 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019), om personen i sina uppgifter kan behandla kunduppgifter eller annars i sina uppgifter kan äventyra funktionen hos informationssystem som är kritiska med tanke på kontinuiteten inom social- och hälsovården. Informationssäkerhetsplanen ska beskriva hur detta säkerställs och hur övriga ovannämnda aspekter beskrivs i avtalen mellan producenten av en informationssystemtjänst och objektet för egenkontroll av informationssäkerheten.

Information om installation, drift och uppdatering av informationssystem ska inkluderas antingen i informationssäkerhetsplanen eller i separata planer som innehåller beskrivningar av processerna för uppdatering, ändringshantering och korrigering. I planerna kan man också beskriva tillvägagångssätten i samband med fel och exceptionella situationer enligt kapitel 6.2. När uppdateringsprocessen beskrivs ska man beakta framför allt versions- och korrigeringsuppdateringar och de förfaranden som andra ändringar eventuellt kräver. Till processen för ändringshantering hör till exempel en beskrivning av förfaranden för testning och godkännande av ändringar i informationssystemen och av nya versioner av systemen. Hanteringen av problem och fel i samband med installation, drift och uppdatering ska tas med i planen.

6.7 Rutiner för hantering av behörigheter och identifiering

Informationssäkerhetsplanen eller de bilagor som den hänvisar till ska beskriva hur åtkomsträttigheterna till kunduppgifter specificeras och administreras, såsom rutiner för uppföljning av behörigheter, identifiering, åtkomsthantering och användning (se kapitel 6.8) inklusive begränsningar. Uppföljningen av användningen ska basera sig på enhetliga yrkesgrupps- och uppgiftsspecifika riktlinjer för behörigheter och användarroller. Informationssystemens användare och olika användargrupper, användarroller och rollernas behörigheter ska beskrivas. Det är viktigt att beskriva hur behörigheterna administreras och i praktiken hanteras med hjälp av klient- eller patientdatasystem eller ett externt informationssystem, till exempel ett identitets- och åtkomsthanteringssystem (IAM). Det är inte nödvändigt att i informationssäkerhetsplanen upprepa de närmare detaljerna om behörigheter, identifieringslösningar eller rollhantering som upprätthålls i sådana externa system.

Informationssäkerhetsplanen ska beskriva hur ändringar i arbetsuppgifterna för anställda inom social- och hälsovården godkänns och dokumenteras i behörigheterna till kunduppgifter[10]. Informationssäkerhetsplanen ska dessutom beskriva vilka personer och roller som har rätt att behandla, avslå och godkänna en begäran om åtkomsträttigheter. Man måste regelbundet gå igenom och följa upp behörigheterna för att säkerställa att de är aktuella.

[10] Social- och hälsovårdsministeriet bereder en förordning om behandling av kunduppgifter inom social- och hälsovården, vars syfte är att komplettera förordningen om åtkomsträttigheter genom att inkludera även åtkomsträttigheter till social- och hälsovårdens gemensamma tjänster och uppgifter som utlämnas mellan social- och hälsovården.

Rutinerna och verksamhetsmodellerna för ansökan om samt beviljande, uppföljning, översyn eller säkerställande och fråntagande av behörigheter ska beskrivas i informationssäkerhetsplanen eller de bilagor som den hänvisar till. I beskrivningarna ska man utöver åtkomsträttigheterna för den egna ordinarie personalen även ange hur åtkomsträttigheterna till nödvändiga kunduppgifter ska ordnas enligt arbetsuppgifterna även för organisationens kortvariga vikarier, studerande som arbetar inom organisationen (med beaktande av begränsningarna för studerande vid yrkesutövning) samt externa tjänsteproducenter (köpta tjänster)[11].

Likaså ska man i informationssäkerhetsplanen eller de bilagor som den hänvisar till beskriva hur, när och på vilket sätt före detta anställda fråntas sina åtkomsträttigheter. Det är särskilt viktigt att beskriva hur åtkomsträttigheterna snabbt kan fråntas enskilda eller flera användarnamn. Det ska föras bok och logg över åtkomsträttigheterna till kunduppgifter och ändringar i dem (se kapitel 6.8).

Informationssäkerhetsplanen eller de bilagor som den hänvisar till ska innehålla en beskrivning av hur man vid objektet för egenkontroll av informationssäkerheten administrerar informationssystemanvändarnas åtkomsträttigheter till funktionerna i Kanta-tjänsterna för elektroniska recept, det riksomfattande patientdataarkivet, klientdataarkivet för socialvården och andra patientuppgifter.

Alla administratörer och informationssystemexperter har som regel inte rätt till kunduppgifter oavsett var kunduppgifterna finns. Ett undantag är felutredningar som gäller lokala register, där administratörer och informationssystemexperter har rätt att granska och korrigera uppgifter om sin egen organisation eller om den organisation för vars räkning de arbetar under utredningen. Även rutiner i samband med detta ska beskrivas i informationssäkerhetsplanen eller i de bilagor som den hänvisar till.

Enligt 8 § i lagen om kunduppgifter ska kunden, tjänstetillhandahållaren, apoteket, andra parter i behandlingen av kunduppgifter och deras företrädare samt de datatekniska enheterna och Kanta-tjänsterna identifieras på ett tillförlitligt sätt vid behandling av kunduppgifter. Informationssäkerhetsplanen ska beskriva identifieringssätten för personer som använder informationssystem (till exempel klient- eller patientdatasystem, apotekssystem, välbefinnandeapplikationer, lokala informationsresurser, datasjöar och läsare) och hanteringen av olika identifieringsverktyg (yrkeskort) samt deras giltighet.

Informationssäkerhetsplanen ska beskriva inloggnings- och identifieringsrutinerna för datorer och mobila enheter samt eventuella lösningar för åtkomsthantering i anslutning till passerkontroll. Lösningarna för lokalernas fysiska säkerhet kan kombineras med de datatekniska säkerhetsrutinerna.

[11] Enligt 9 § 3 mom. i lagen om kunduppgifter ska tjänstetillhandahållare och apotek specificera åtkomsträttigheterna till kunduppgifter inom social- och hälsovården för alla de arbetstagare vars arbetsuppgifter förutsätter behandling av kunduppgifter. Åtkomsträttigheterna ska specificeras så att respektive arbetstagare endast har åtkomst till de kunduppgifter som är nödvändiga för genomförandet av arbetsuppgifterna.

Informationssäkerhetsplanen ska beskriva vilka system, uppgifter, enheter eller situationer som kräver multifaktorautentisering (Multi-Factor Authentication, MFA) och i synnerhet identifiering med yrkeskort med hjälp av certifikat för social- och hälsovården för att säkerställa kunduppgifternas konfidentialitet och integritet[12].

Informationssystem som behandlar patientuppgifter eller klientuppgifter inom socialvården, oberoende av om systemet är kopplat till Kanta-tjänsterna, får inte använda gemensamma användarnamn för funktioner för redigering eller visning av kunduppgifter eller funktioner för elektroniska recept.

Inloggning i Kanta-tjänsterna förutsätter stark elektronisk autentisering. Tillförlitlig elektronisk identifiering av personer som arbetar inom social- och hälsovården sker med certifikat för yrkeskort för social- och hälsovården. Rutiner för hantering av dessa ska beskrivas i informationssäkerhetsplanen.

Användarens identitet ska alltid verifieras innan åtkomsträttigheter eller identifieringsverktyg beviljas. Metoden för verifiering och autentisering ska beskrivas i informationssäkerhetsplanen.

Informationssäkerhetsplanen ska beskriva användningen av eventuella gemensamma användarnamn[13].

Fleranvändarvyer med identifierbara kunduppgifter kan användas till exempel i en samlingsvy över patientplatser vid en avdelning eller i motsvarande patientadministrativa icke-behandlingssyften som är nödvändiga för att utföra arbetet i praktiken. Informationssäkerhetsplanen ska beskriva hur sådana uppgifter och vyer skyddas mot utomstående till exempel genom lokal- och passerhanteringslösningar i olika praktiska situationer i samband med behandling av kunduppgifter. Dessutom ska man kunna bevisa i efterhand, till exempel genom lösningar för skifthantering eller åtkomsthantering, vilka anställda som använder sådan information i sitt arbete[14].

6.8 Rutiner för uppföljning av åtkomsthantering och användning av klient- och patientdatasystem

Med de logguppgifter som samlas in från informationssystemen följer man upp användningen och utlämnandet av uppgifter i enlighet med 10 § i lagen om kunduppgifter och utreder tekniska systemfel i myndigheternas verksamhet enlighet med 17 § i informationshanteringslagen. I 17 § i informationshanteringslagen föreskrivs om myndigheternas skyldighet att samla in logguppgifter. Eftersom även privata tjänstetillhandahållare ansluter sig som användare av de riksomfattande informationssystemtjänsterna innehåller lagen om kunduppgifter bestämmelser om uppföljning av användningen och utlämnandet av uppgifter så att samma skyldigheter gäller alla tjänstetillhandahållare inom social- och hälsovården. Uppföljningen av användningen och utlämnandet regleras i lagen om kunduppgifter på en mer detaljerad nivå än i informationshanteringslagen.

Processerna för att skapa och behandla logguppgifter i anslutning till användningen av klientuppgifter ska syfta till att skapa nödvändiga loggar som förblir oförändrade och beviskraftiga.

---

[12] Identifiering med användarnamn och lösenord kan endast användas vid behandling av kunduppgifter som sker lokalt i klient- och patientdatasystem hos objektet för egenkontroll av informationssäkerheten.

[13] Användningen av gemensamma användarnamn är tillåten i situationer där man granskar organisationens resursanvändning eller andra icke-identifierande uppgifter om processer som inte gäller enskilda personer eller sammanfattande uppgifter om flera kunder.

[14] Dataskyddslagen 1050/2018 6 § 2 mom. 1 punkten: ”...åtgärder för att det i efterhand ska kunna säkerställas och bevisas vem som har registrerat, ändrat eller överfört personuppgifter; ...”.

En tjänstetillhandahållare ska för uppföljningen och tillsynen samla in logguppgifter från varje kundregister om all användning och allt utlämnande av kunduppgifter (10 § i lagen om kunduppgifter), om användningen av informationssystemet förutsätter identifiering eller annan inloggning. Apoteken ska samla in användningslogguppgifter om behandlingen av recept och andra anteckningar om läkemedelsbehandling som lagrats i receptcentret[15].

Objektet för egenkontroll av informationssäkerheten ska följa upp och övervaka att uppgifterna i klient- och patientdatasystemen, patientdataarkivet, klientdataarkivet för socialvården och receptcentret endast kan visas och behandlas av behöriga personer. Uppföljningen av användningen ska basera sig på enhetliga yrkesgrupps- och uppgiftsspecifika riktlinjer för behörigheter och användarroller (se kapitel 6.7).

Objektet för egenkontroll av informationssäkerheten ska ha en plan för uppföljning och övervakning av dataskyddet och behandlingen av kunduppgifter samt genomförandet av informationssäkerhetsplanen och den kan också ingå i informationssäkerhetsplanen. Det är fråga om en uppföljnings- och övervakningsplan med vilken man följer upp användningen av personuppgifter och informationssystem. I uppföljnings- och övervakningsplanen ska man åtminstone ta ställning till hur man regelbundet följer upp användningen av personuppgifter och hur man går till väga i situationer där missbruk förekommer. Uppföljnings- och övervakningsplanen ska beskriva tillvägagångssätt om fel, misstankar om förseelser eller obehörig användning av kunduppgifter avslöjas i användningslogguppgifterna. Uppföljnings- och övervakningsplanen ska också beskriva hur den personuppgiftsansvarige och FPA ska agera när de lämnar ut uppgifter från utlämningsloggregistret[16].

Uppföljnings- och övervakningsplanen kan till exempel vara årsspecifik. Det är viktigt att regelbundet granska och vid behov uppdatera planen. Egenkontrollen av dataskyddet och användningen av kunduppgifter genomförs i praktiken via planen. Vid rapporteringen om övervakningen av användningen av kunduppgifter rekommenderas att man tillämpar metoden för databokslut eller en annan motsvarande årlig rapportering, som också kan användas för att uppfylla den personuppgiftsansvariges ansvarsskyldighet enligt EU:s allmänna dataskyddsförordning.

Organisationens interna uppföljning och rapportering av logguppgifter bör inbegripa en regelbunden detaljerad uppföljning och övervakning av kunduppgifter som behandlats i organisationen och av användare som är verksamma där, inklusive observationer av eventuella informationssäkerhetsincidenter. Detaljerade rutiner för uppföljning av hanteringen och användningen av loggar ska beskrivas antingen i informationssäkerhetsplanen eller i separata dokument. Sådana rutiner är till exempel hur man besvarar kunders och myndigheters begäran om information, sammanställer och hanterar loggrapporter samt rollerna för personer som deltar i tillsynsverksamheten. Mer information finns i kapitlet om rapporteringskrav i de nationella kravspecifikationerna för hantering av logguppgifter17.

---

[15] 10 § i lagen om kunduppgifter, 3 § i lagen om elektroniska recept 61/2007.

[16] Ansvarsfördelningen i anslutning till ärendet beskrivs i bilagan till förbindelsen angående kundrelationen till Kanta-tjänsterna (1.1.2024): ”Beskrivning av det gemensamma personuppgiftsansvaret för tjänster i anslutning till Kanta-tjänsterna”.

[17] Asiakas- ja potilastietojen käsittelyssä syntyvien lokitietojen hallinnan kansalliset vaatimusmäärittelyt v 1.2 (endast på finska)

6.9 Fysisk säkerhet som en del av säkerheten i informationssystemens driftmiljö

Objektet för egenkontroll av informationssäkerheten ska i informationssäkerhetsplanen beskriva hur man beaktar den fysiska driftmiljön där kunduppgifter behandlas. Detta kan till exempel innebära att man undersöker olika typer av lokaler samt relaterade åtgärder för lokalutformning, inredning, ljudisolering eller andra motsvarande åtgärder som i praktiken kan påverka dataskyddet och informationssäkerheten. Informationssäkerhetsplanen ska också beskriva hur man sörjer för den fysiska säkerheten i servrarnas driftmiljö.

Informationssäkerhetsplanen ska beskriva hur skärmar, arbetsstationer och skrivare är placerade och skyddade mot utomstående för att säkerställa en informationssäker driftmiljö. Till helheten hör teknisk och fysisk passerkontroll och eventuella åtgärder för att begränsa den fysiska åtkomsten. Informationssäkerhetsplanen ska på en allmän nivå beskriva hur dessa faktorer har beaktats och var det finns mer detaljerad information vid behov.

Informationssäkerhetsplanen ska beskriva hur objektet för egenkontroll av informationssäkerheten har ombesörjt och verifierat dataskyddet och informationssäkerheten för eventuella mobila enheter som innehåller kunduppgifter.

Informationssäkerhetsplanen ska beskriva hur man hanterar och skyddar användningen av externa lagringsmedier både för den egna personalen och för obehöriga.

Det ska finnas beskrivningar av hur kunduppgifter som skrivs ut på papper från informationssystemen förvaras och förstörs på lämpligt sätt, så att obehöriga inte får tillgång till kunduppgifter från objektet för egenkontroll av informationssäkerheten. Användning av säkerhetsutskrifter rekommenderas i stället för traditionella utskriftslösningar.

Informationssäkerhetsplanen ska beskriva hur man säkerställer att arkiveringsenheten har en fysisk verksamhetsmiljö som är brandsäker, ändamålsenlig och tillräckligt rymlig med tanke på dess uppgifter. Informationssäkerhetsplanen ska beskriva hur rutinerna för förstöring av utskrifter som innehåller kunduppgifter har planerats och genomförts samt hur alla anställda som behandlar utskrifter som innehåller kunduppgifter har utbildats i dessa rutiner. Informationssäkerhetsplanen ska beskriva hurudana anvisningar personalen ges för att förstöra icke-offentliga och sekretessbelagda pappersutskrifter samt hur detta möjliggörs i praktiken med tillräckligt många låsbara förvaringsbehållare och/eller så kallade korsskärande dokumentförstörare med tillräcklig säkerhetsklass, vilka lämpar sig för ändamålet.

6.10 Hantering av datorer, mobila enheter och stödtjänster för driftmiljön

Informationssäkerhetsplanen ska beskriva hur man i informationssystemens driftmiljö på ett informationssäkert sätt sörjer för hanteringen av de datorer och mobila enheter som klient- och patientdatasystemen använder. Dessutom ska man beskriva hur man går till väga för att radera uppgifter från enheter som använts av arbetstagare vars anställningsförhållande har upphört. Informationssäkerhetsplanen eller tillhörande dokument ska beskriva hur man i praktiken säkerställer att programmen som skyddar enheter och tjänster mot virus och skadliga program fungerar och uppdateras samt hur man har ordnat övriga säkerhetsrutiner, till exempel användarnamn, lösenord, PIN-koder, hanteringen av SIM-kort samt fjärrlåsning och/eller tömning av försvunna mobila enheter.

Dessutom ska informationssäkerhetsplanen beskriva hur man ordnar allmänna stödtjänster för driftmiljön, till exempel uppdateringar av operativsystem och systemprogram (till exempel MS Office). Till helheten hör eventuella härdningar samt säkerställande av operativsystemets och systemprogrammens interoperabilitet och uppföljning av hur de fungerar tillsammans med informationssystemen för social- och hälsovården.

Det är viktigt att informationssäkerhetsplanen och/eller dess bilagor beskriver driftmiljön som helhet åtminstone i fråga om tidigare nämnda faktorer. Ansvars- och arbetsfördelningsfrågorna ska tydligt framgå av beskrivningen, det vill säga vilka frågor tjänstetillhandahållarens egen verksamhet respektive avtalsparterna ansvarar för. Eventuella producenter av utkontrakterade tjänster ska också beskrivas. Faktorerna ska formuleras tillräckligt noggrant i avtalen mellan aktörerna för att säkerställa en informationssäker och smidig verksamhet.

6.11 Informationssäker användning av plattforms- och webbtjänster med tanke på dataskyddet och beredskapen

Objektet för egenkontroll av informationssäkerheten måste vara medveten om alla plattforms- och webbtjänster som den använder och det ska framgå vilka tjänster objektet för egenkontroll av informationssäkerheten själv ansvarar för, vilka tjänster producenten av en informationssystemtjänst som agerar för dennes räkning ansvarar för och vilka tjänster en eventuell tredje part ansvarar för.

Följande underpunkter a–j förpliktar objektet för egenkontroll av informationssäkerheten att i informationssäkerhetsplanen eller i de bilagor som den hänvisar till beskriva eller åtminstone ta ställning till hur det som beskrivs i underpunkten säkerställs med de plattforms- och webbtjänster som används i driftsmiljön hos objektet för egenkontroll av informationssäkerheten. Dessa aspekter ska särskilt beaktas och säkerställas i avtal mellan objektet för egenkontroll av informationssäkerheten och producenten av en informationssystemtjänst:

a) Hur säkerställer man att dataskyddsbestämmelserna, till exempel den allmänna dataskyddsförordningen, följs? Överföring och förvaring av personuppgifter inom EU/EES-området är i regel tillåten med motsvarande skyddsåtgärder som i Finland. Risknivån för överföring av uppgifter måste bedömas (konsekvensbedömning enligt den allmänna dataskyddsförordningen). Om uppgifter överförs utanför EU/EES-området till s.k. tredjeländer, ska de i lagstiftningen fastställda, godkända grunderna för överföring av personuppgifter iakttas och nödvändiga organisatoriska, avtalsbaserade och tekniska skyddsåtgärder vidtas från fall till fall och i varje land. Ytterligare aktuella upplysningar finns på webbplatsen för Dataombudsmannens byrå under Överföring av personuppgifter till länder utanför Europeiska ekonomiska samarbetsområdet[18].

b) Hur har informationssäkerhetsåtgärderna för både servrar och de driftmiljöer som dessa förutsätter, till exempel skyddet av datanätet samt duplicerings-, drift- och underhållsåtgärder, ordnats?

c) Hur sörjer man för de praktiska arrangemangen i datakommunikationsfrågor, tillgången till tjänster, ordnandet av informationssäkerhetsrutiner för näten, uppdateringen och informationssäkerheten för nätverksenheter och deras komponenter, programvara samt trådlösa nätverk och routrar, anvisningar för fjärranslutning och distansarbete samt fjärradministrationslösningar? Kraven på dataskydd och informationssäkerhet för datakommunikation och informationsförmedling och fastställandet av ansvar ska utgöra en del av avtalet mellan objektet för egenkontroll av informationssäkerheten och datakommunikations- eller informationsförmedlingsoperatören.

d) Hur underhålls informationssystemen och deras driftmiljöer och hur förbereder man sig på att agera i undantagssituationer där informationssystemen inte är tillgängliga?

e) Hur hanterar och administrerar man befintliga lösningar, avtal och rutiner? Sådana är till exempel molnbaserade lösningar, fjärradministrationstjänster, serveruthyrning, serverhantering, backuptjänster och datorhallstjänster.

f) Hur skyddas större dataset med känsliga och sekretessbelagda kunduppgifter så att obehöriga inte har tillgång till okrypterade kunduppgifter? Vid omfattande förvaring av kunduppgifter ska tjänstetillhandahållaren och/eller producenten av en informationssystemtjänst ha krypteringsnycklar om uppgifterna förmedlas eller överförs till tredjepartstjänster. Leverantören av en plattformstjänst och/eller driftmiljön som den ansluts till får inte ha tillgång till krypteringsnycklarna.

[18] https://tietosuoja.fi/sv/overforing-av-personuppgifter-till-lander-utanfor-ees

g) Hur förbereder man sig på att behandla uppgifter under förhållanden som avviker från det normala inom kritiska tjänster? Kritiska tjänster är till exempel den offentliga hälso- och sjukvårdens tjänster med jouransvar. I beredskapen ska man beakta de största riskerna i situationer där samhällets nätförbindelser är begränsade till Finlands geografiska gränser (till exempel informationshantering i dessa situationer). Dessutom bör beredskapen omfatta planering av alla lämpliga datatekniska och icke-datatekniska metoder (till exempel möjligheten att tillfälligt använda kulspetspennor och häften för registrering av patientuppgifter) samt rutiner för överföring av uppgifter till informationssystemen när förhållandena tillåter det.

h) Hur regelbundet följs plattforms- och webbtjänster upp bland annat med tanke på funktionalitet, informationssäkerhetsrisker, störningssituationer och ändringar i användarvillkoren? Vid behov ska avtal och rutiner uppdateras så att de motsvarar den förändrade situationen.

i) Hur har man ordnat planen för informationssystem, delsystem, utrustningskomponenter och nätverk samt underhåll, uppdatering och förnyelse, liksom en tydlig strategi för beslutsfattandet i anslutning till underhållsåtgärderna? Hur följer man upp behoven av att uppdatera dessa?

j) Hur har man sett till att informationssystemen uppfyller de väsentliga informationssäkerhetskraven som ställs på dem, även till den del som genomförandet eller användningen av systemen stöder sig på plattforms- eller kapacitetstjänster från tredje part?

6.12 Informationssäkerhetsrutiner för anslutning till Kanta-tjänsterna och användning av dem

Informationssäkerhetsplanen ska innehålla en redogörelse för hur man säkerställer de krav som en informationssäker användning av de riksomfattande informationssystemtjänsterna förutsätter när en tjänstetillhandahållare eller ett apotek håller på att ansluta sig som användare av Kanta-tjänsterna. Uppfyllandet av kraven för Kanta-tjänsterna ska beskrivas i informationssäkerhetsplanen eller i de bilagor som den hänvisar till och ska kunna verifieras i tillsynssituationer som ordnas av tillsynsmyndigheten.

Tjänstetillhandahållare och apotek ska se till att personalen behärskar verksamhetsmodellerna och principerna för användning av Kanta-tjänsterna samt känner till följderna av missbruk. Informationssäkerhetsplanen ska beskriva hur tjänstetillhandahållaren och apoteket verifierar att kunderna informeras om Kanta-tjänsterna och användningen av kunduppgifter.

Informationssäkerhetsplanen ska beskriva hur användningen av Kanta-tjänsterna har beaktats i personalens utbildningsmaterial, utbildningar och anvisningar (7 § i lagen om kunduppgifter).

Tjänstetillhandahållaren ska beskriva sin verksamhetsmodell för att aktivt följa upp användningen av Kanta-tjänsterna. Som en del av verksamhetsmodellen ska det bland annat finnas en beskrivning av hur man kontrollerar att handlingar arkiveras korrekt[19] och de felmeddelanden som Kanta-tjänsterna skickar.

Tjänstetillhandahållaren ska dessutom säkerställa att endast patient- och klienthandlingar som hör till social- och hälsovårdens register eller andra handlingar som innehåller kunduppgifter samt handlingar som handlingar som hänför sig till ordnandet av social- och hälsovården arkiveras i Kanta-tjänsterna (69 § i lagen om kunduppgifter).

---

[19] Enligt lagen om kunduppgifter ska en kundhandling utan dröjsmål upprättas och föras in i Kanta-tjänsterna när handlingen är klar (21 § och 65 § i lagen om kunduppgifter). Fördröjningar i arkiveringen eller att handlingar inte arkiveras kan medföra betydande risker för uppgifternas integritet, patient- och klientsäkerheten, klienternas rättigheter samt rättsskyddet för yrkesutbildade personer inom social- och hälsovården.

Tjänstetillhandahållare och apotek ska ha tydliga tillvägagångssätt och en tydlig ansvarsfördelning för att upptäcka, informera om, åtgärda och följa upp störningar och fel i Kanta-tjänsterna och system som är anslutna till dem. Avtalen mellan tjänstetillhandahållaren och producenten av en informationssystemtjänst eller mellan apoteket och producenten av en informationssystemtjänst ska innehålla en beskrivning av ansvaret för tillvägagångssätten samt arbetsuppgifterna för behandling av logguppgifter i händelse av störningar eller kränkningar av informationssäkerheten. Man ska komma överens om till exempel rutinerna för kund- och myndighetskommunikation och nödvändiga förfaranden för behandling av händelselogguppgifter.

Informationssäkerhetsplanen ska beskriva hur den tekniska supporten för Kanta-tjänsterna får kännedom om tjänstetillhandahållarens och apotekets ansvariga parter vid störningar. Ändringar i de informationssystem som tjänstetillhandahållaren och apoteket använder (inklusive versionsuppgifter eller andra uppgifter som beskriver informationssystemets status) ska anmälas till FPA enligt dess anvisningar. Kanta-tjänsterna fungerar som personuppgiftsbiträde och stöder den personuppgiftsansvariges tekniska utredningar av störningar, fel och intrång.

Tjänstetillhandahållare och apotek ska i informationssäkerhetsplanen beskriva hur användningen av kunduppgifter som hämtats från Kanta-tjänsterna följs upp. Detta gäller i synnerhet hur uppföljningen av användningen av så kallad nödsökning organiseras, sökning och användning av särskilt känsliga uppgifter samt sökningar som gjorts utan teknisk verifiering av vårdrelationen (så kallad särskild anledning). Personalen ska vara medveten om uppföljningen och följderna av missbruk.

Tjänstetillhandahållare och apotek ska säkerställa att det informationssystem som anskaffas eller uppdateras för dess verksamhet uppfyller de väsentliga krav som motsvarar informationssystemets användningsändamål i enlighet med THL:s föreskrift 5/2024. Tjänstetillhandahållare och apotek ska regelbundet följa upp att informationssystem och informationsförmedlingsservice som hör till klass A1, A2 eller A3 enligt THL:s föreskrift 4/2024 har ett giltigt intyg över bedömning av informationssäkerheten. (Jfr kapitel 6.5)

I fråga om informationssystem som ska anslutas till Kanta-tjänsterna (särskilt system i klass A2 eller A3) ska man säkerställa att de egenskaper som motsvarar systemets användningsändamål har samtestats med godkänt resultat (jfr kapitel 6.5. Dessa uppgifter är offentligt tillgängliga i Valviras register över informationssystem. Dessutom ska tjänstetillhandahållaren eller apoteket säkerställa att även andra informationssystem än de som ansluts till Kanta-tjänsterna och som är avsedda för behandling av klientuppgifter inom socialvården och patientuppgifter har anmälts till Valvira och att uppgifterna i Valviras register över informationssystem är aktuella. Om välbefinnandeapplikationer används i tjänstetillhandahållarens verksamhet, ska motsvarande säkerställanden göras även i fråga om dem.

Tjänstetillhandahållare och apotek ska också fastställa tillvägagångssätten för praktiska verksamhets- och ansvarsfrågor i situationer där ett intyg om bedömning av informationssäkerheten för ett informationssystem eller för informationsförmedlingsservice återkallas för viss tid eller helt och hållet eller där användningen av informationssystemet förbjuds eller begränsas. Sådana faktorer ska beaktas på förhand i avtal mellan tjänstetillhandahållare, apotek, mellanhänder och producenter av informationssystemtjänster (jfr THL:s föreskrift 5/2024).

7 Handledning och rådgivning

Institutet för hälsa och välfärd ger på begäran råd och handledning om tillämpningen av denna föreskrift och tillhandahåller vid behov en mall för informationssäkerhetsplanen.

8 Ikraftträdande

Denna föreskrift träder i kraft den 22 februari 2024 och gäller tills vidare. Tjänstetillhandahållare, apotek, mellanhänder och Folkpensionsanstalten ska uppdatera sina tidigare informationssäkerhetsplaner som gäller dataskydd, informationssäkerhet och användningen av informationssystem så att de överensstämmer med denna föreskrift.

Sirpa Soini
direktör

Jarmo Kärki
enhetschef

Bilaga

Mall för en informationssäkerhetsplan

För kännedom

Tjänstetillhandahållare inom social- och hälsovården
Apotek
Mellanhänder
Folkpensionsanstalten

Dataombudsmannens byrå
Säkerhets- och utvecklingscentret för läkemedelsområdet Fimea
Tillstånds- och tillsynsverket för social- och hälsovården Valvira
Regionförvaltningsverken

Social- och hälsovårdsministeriet
Traficom/Cybersäkerhetscentret
Finansministeriet
Myndigheten för digitalisering och befolkningsdata

Kompetenscentrum inom det sociala området
Hyvinvointialueyhtiö Hyvil Oy

Denna föreskrift publiceras i myndigheternas föreskriftssamlingar

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

och finns att tillgå:

- på registratorskontoret vid Institutet för hälsa och välfärd samt på
- webbaddressen https://thl.fi/aiheet/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset