Tillitsramverk – Fedvis

Bakgrund

Kraven i detta tillitsramverk syftar till att uppfylla ”Lag om Nationella läkemedelslistan, 2018:1212, 8 kap 2 §.

Kraven under avsnitt ”A” i detta Tillitsramverk är harmoniserade med ”HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården”. Part som lyder under denna föreskrift kan därigenom förenkla sin deklaration om efterlevnad av Tillitsramverket genom att beskriva följsamhet mot angivna paragrafer under respektive avsnitt.

A. Generella krav

Säkerhetsarbete

A.0 Betrodd Part ska för den Funktion (VIS, Vårdinformationssystem) som Tillitsdeklarationen avser intyga följsamhet mot kraven i detta Tillitsramverk avseende:

a) Betrodd Part ska ha infört ett ledningssystem för informationssäkerhet för att säkerställa tillgänglighet, riktighet, konfidentialitet och spårbarhet av personuppgifter. Ledningssystemet ska innehålla en övergripande informationssäkerhetspolicy och det ska vara baserat på genomförda riskanalyser. Ledningssystemet bör följa standarderna i ISO/IEC 27000-familjen.
(3 kap. 1 §, 2 §, 4 §, 5 §)

b) Betrodd Part ska ha infört en organisation för informationssäkerhetsarbetet, inkluderande en utsedd ansvarig. Informationssäkerhetsarbetet ska innefatta en årlig genomgång av incidenter, riskanalys, skyddsutvärdering och förbättringsarbete.
(3 kap. 6 §, 18§~~)~~

c) Betrodd Part ska säkerställa skydd av personuppgifter vid utveckling eller upphandling av informationssystem för dessa, liksom fysiskt skydd.
(3 kap. 9 §, 10 §, 14 §)

d) Betrodd Part ska skydda personuppgifter vid överföring i öppna nät och vid elektronisk åtkomst. Stark autentisering ska användas.

(3 kap. 15 §)

A.1 Betrodd Part ska tilldela individuella behörigheter för åtkomst till personuppgifter, baserade på behov och risk. Det ska finnas rutiner för ändring och borttagning av behörigheter, samt för uppföljning av dessa.
(4 kap. 2 §, 3 §~~)~~

A.2 Betrodd Part ska ansvara att personal skyddar lösenord, hjälpmedel för autentisering och datorer mot att användas för obehörig åtkomst. Detta gäller även för inhyrd eller kontrakterad personal.
(6 kap. 1 §, 2 §)

A.3 Betrodd Part ska säkerställa att Patientsäkerhetsberättelsen innehåller en sammanställning av informationssäkerhetsarbetet enligt A.0 b).
(7 kap. 1 §).

A.4 Eventuella avvikelser från föreskrifternas krav ska specificeras med en notering om planerad tid för åtgärd.

Kryptografisk säkerhet

A.5 Betrodd Part ska skydda Funktionen mot obehörig åtkomst och skydda kryptografiskt nyckelmaterial, omfattande minst signeringsnycklar för:
a) metadata
b) identitetsintyg
c) kommunikationskanal för Identitetsintyg

Ansvar för användning av leverantörer

A.6 Betrodd part som, i delar eller i helhet, lägger ut utförande av Funktionen på leverantör är, oavsett avtalsform, ansvarig för leverantörens uppfyllande av kraven i Tillitsramverket.

Informationsplikt

A.7 Betrodd Part ska informera E-hälsomyndigheten vid incidenter som kan riskera tilliten till organisationens anslutning, samt vid ändringar av kontaktpersoner och metadata.

B. E-legitimationsutfärdare

B.1 E-legitimationsutfärdare ska vara godkänd av Myndigheten för digital förvaltning (DIGG) i enlighet med Tillitsramverket för Svensk e-legitimation.

C. Identitetsintygsutgivare

C.1 Betrodd Part som ställer ut Identitetsintyg ska se till att utlämnande av Identitetsintyg föregås av en tillförlitlig kontroll av att den angivna Användarens elektroniska identitet och Attribut är giltiga.

C.2 Tillitsnivå för autentisering av användaren ska anges i identitetsintyget. Hur tillitsnivå anges och tolkas ska följa specifikation från Myndigheten för digital förvaltning (DIGG).

C.3 Lämnade Identitetsintyg får vara giltiga i upp till 60 minuter.

C.4 Informationen i identitetsintyg ska skyddas mot obehörig åtkomst.

C.5 Identitetsintyg ska utfärdas på ett sådant sätt så att mottagaren kan kontrollera att intyget är oförvanskat och utfärdat av rätt avsändare.

C.6 Identifierad Användares inloggningssession mot intygsutgivningstjänsten ska tidsbegränsas, varefter en ny identifiering av Användaren ska ske i enlighet med C.1.

Ändringslogg		
Version	**Datum**	**Kommentar**
V1.0.	2024-02-28	Första version.