# 7.2 Fælles standarder for sikker udveksling af information

4. maj 2016

**Aftalens indhold**

Der har været en stigende efterspørgsel fra myndighederne efter at koordinere og sammentænke brugerstyring på tværs af den offentlige sektor, og der er gennem de senere år blevet udviklet fællesoffentlige standarder som fx OIOIDWS, der blandt andet gør det muligt at vise personlige data fra offentlige registre på en sikker og standardiseret måde. Skiftet til fællesoffentlige standarder er undervejs flere steder i den offentlige sektor og er en væsentlig trædesten for fremtidig digitalisering.

Med implementeringen af telemedicin, herunder digitale velfærdsløsninger i borgernes hjem samt patientrapporterede oplysninger (PRO), begynder sundhedsvæsenet i stor skala at tilbyde digitale løsninger til borgere og patienter. Der indsamles helbredsoplysninger via måleudstyr i hjemmet, og borgerne besvarer spørgeskemaer digitalt. Denne positive udvikling udfordrer imidlertid visse af de sikkerhedsstandarder, som i dag benyttes.

Sikkerhedsstandarderne skal derfor opdateres ved at sikre, at fællesoffentlige sikkerhedsstandarder såsom OIOIDWS i stigende grad benyttes. Dette vil gøre det nemmere at udbygge digitaliseringen af fx sundhedsvæsenet med tidssvarende teknologiske løsninger og samtidig gøre det nemmere for it-leverandører at byde ind med moderne - og måske billigere - it-løsninger, når der ikke stilles krav om, at it-løsninger skal anvende en særlig domænespecifik sikkerhedsstandard, som til og med forekommer mere og mere teknologisk utidssvarende.

Sundhedsvæsenets parter, herunder kommunerne, har i forbindelse med implementeringen af Fælles Medicinkort (FMK) investeret i sikkerhedshåndtering målrettet sundhedsområdet. Denne "system-til-system sikkerhed" har været nødvendig og er fortsat relevant for brugen af FMK mv. Med initiativet om fælles it-sikkerhedsstandarder i den offentlige sektor sikres det imidlertid, at kommuner og regioner fremadrettet i højere grad kan genbruge fællesoffentlige sikkerhedsstandarder.

Parterne på sundhedsområdet gennemførte i 2014 i regi af den Nationale Strategi for Digitalisering af Sundhedsvæsenet 2013-2017 en omfattende analyse af mulighederne for at samordne forskellige sikkerhedsstandarder, herunder muligheden for at overgå fra brugen af "den gode webservice" til den fællesoffentlige OIOIDWS-sikkerhedsstandard. Analysen viste, at det er muligt at gennemføre dette skift, og at det vil være hensigtsmæssigt at gennemføre en række konkrete afprøvninger samt udarbejde en migreringsplan for de systemer, det anses for relevant at omlægge til en fælles sikkerhedsstandard.

Initiativet består af følgende elementer:

1. Opdatering af infrastrukturen med henblik på at kunne teste sikkerhedsstandarderne i blandt andet elektroniske patientjournaler, omsorgsjournaler mv.
2. Afprøvning den fællesoffentlige standard OIOIDWS på sundhedsområdet.
3. På baggrund af testene estimeres de fremadrettede omkostninger ved ibrugtagning af de nye sikkerhedsstandarder i relevante it-systemer.
4. Fastlæggelse af fremtidige samarbejdsforpligtelser omkring OIOIDWS.
5. Udarbejdelse af en migreringsplan for, hvilke it-systemer der bør omlægges og/eller opdateres til at kunne anvende de nye sikkerhedsstandarder. Migreringsplanen tiltrædes af Den nationale bestyrelse for sundheds-it, jf. *Organisering*.

**Organisering**

Initiativet kræver et tæt samarbejde mellem sundhedsvæsenet og Digitaliseringsstyrelsen. Sidstnævnte er standardejer på den fællesoffentlige OIOIDWS-sikkerhedsstandard. Initiativet forankres i Den nationale bestyrelse for sundheds-it. På baggrund af resultatet af initiativets punkt 1-3 forelægges beslutningsoplæg om gennemførelse af punkt 4-5 for bestyrelsen. Der afrapporteres på initiativets fremdrift til porteføljestyregruppen for den fællesoffentlige digitaliseringsstrategi i overensstemmelse med de aftalte governance- samt økonomi- og porteføljestyringsprincipper. Initiativets gennemførelse koordineres med initiativ 7.3 *Digitale identiteter og rettighedsstyring*.