MINISTERIET FOR SUNDHED OG FOREBYGGELSE

Holbergsgade 6
DK-1057 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Dato: 20. januar 2015
Enhed: Sundhedsøkonomi
Sagsbeh.: SUMCBM
Sags nr.: 1404754
Dok. nr.: 1628329

Rigsrevisor
St. Kongensgade 45, 4. sal
1264 København K

Vedr. Statsrevisorernes beretning nr. 1/2014 om statens behandling af fortrolige oplysninger om personer og virksomheder

Under henvisning til Statsrevisorernes brev af 20. november 2014 (Ref. 14-000917-16) kan Ministeriet for Sundhed og Forebyggelse skal Ministeriet for Sundhed og Forebyggelse bemærke følgende:

Rigsrevisionens undersøgelse om statens behandling af fortrolige oplysninger om personer og virksomheder blev, for så vidt angår Sundhedsstyrelsen, udført i relation til to it-systemer:

- Udleveringstilladelser (ULS), der understøtter Sundhedsstyrelsens behandling af ansøgninger fra læger, dyrlæger og tandlæger om udlevering af lægemidler, der ikke er markedsført i Danmark. Systemet er relateret til fortrolige oplysninger om personer.
- Kategorisering Af Totaloplysninger om lægemidler (KAT), der er et fagsystem, som anvendes i forbindelse med godkendelse og markedsføring af lægemidler. Systemet er relateret til fortrolige oplysninger om virksomheder.

I det følgende gennemgås de initiativer, som Sundhedsstyrelsen har iværksat i relation til de kritikpunkter, som Rigsrevisionen har anført i beretningen.

Ad beretningens punkt 2: Institutionernes beskyttelse af fortrolige oplysninger
Ad beretningens punkt 2.1: Institutionernes beskyttelse af fortrolige oplysninger om personer
Retningslinjer
Det fremgår af beretningen:

- At Sundhedsstyrelsen mangler enkelte specifikke retningslinjer.
- At Sundhedsstyrelsen ikke har opdateret alle it-sikkerhedsmæssige retningslinjer inden for det seneste år.

Det kan hertil bemærkes, at Sundhedsstyrelsen inden udgangen af 2014 har udarbejdet de manglende retningslinjer, herunder de retningslinjer for distancearbejdspladser, som er specifikt nævnt i beretningen. Sundhedsstyrelsen indfører derefter med virkning fra 1. marts 2015 procedurer, der sikrer, at alle de interne retningslinjer bliver gennemgået mindst én gang om året.

Brugeradgange og kontrol heraf
Det er i beretningen anført:

- At Sundhedsstyrelsen har defineret, hvem der må have adgang til det undersøgte system, og har godkendt de pågældendes autorisationer.
- At Sundhedsstyrelsen ikke udfører halvårlig kontrol af, om brugerne (stadig) har et arbejdsbetinget behov for at have adgang til systemet.

Ministeriet kan oplyse, at Sundhedsstyrelsen har indgået aftale med it-driftsleverandøren af det omhandlede system (databehandleren) om, at denne to gange årligt igangsætter en proces, hvorefter den systemansvarlige i Sundhedsstyrelsen gennemgår og godkender brugernes adgangsrettigheder til systemet. Denne proces er imidlertid ikke forløbet tilfredsstillende, hvorfor Sundhedsstyrelsen har skærpet overvågningen af, at processen igangsættes og gennemføres til tiden.

Det er Sundhedsstyrelsens forventning, at kontrollen af brugeradgange fra og med 1. marts 2015 fungerer i fuld overensstemmelse med reglerne i sikkerhedsbekendtgørelsen.

Kontrol af afviste adgangsforsøg
Det fremgår af beretningen:

- At Sundhedsstyrelsen registrerer afviste forsøg på at få adgang til systemet.
- At Sundhedsstyrelsen låser systemet, hvis der forekommer flere forgæves forsøg på at få adgang.
- At Sundhedsstyrelsen ikke følger regelmæssigt op på, om der har været afviste forsøg.

Det kan oplyses, at Sundhedsstyrelsens it-driftsleverandør hver måned gennemgår alle uautoriserede adgangsforsøg, ligesom Sundhedsstyrelsen via månedsrapporter fra it-driftsleverandøren bliver orienteret om adgangsforsøgene.

Sundhedsstyrelsen mangler imidlertid interne retningslinjer om, hvordan og ud fra hvilke kriterier, der følges op på adgangsforsøgene. Retningslinjer herom vil blive udarbejdet inden 1. marts 2015.

Registrering af opslag på enkeltpersoner
Det fremgår af beretningen:

- At Sundhedsstyrelsen registrerer medarbejdernes opslag på enkeltpersoner.
- At Sundhedsstyrelsen ikke sletter registreringerne efter 6 måneder.

Ministeriet kan oplyse, at Sundhedsstyrelsen efter Rigsrevisionens gennemførte undersøgelse har ændret praksis, således at registreringerne nu – i overensstemmelse med sikkerhedsbekendtgørelsen – slettes efter 6 måneder.

Aftaler med databehandlere
Det fremgår af beretningen:

- At Sundhedsstyrelsen har indgået skriftlig aftale med databehandleren med det fornødne indhold.

- At Sundhedsstyrelsens indhentede revisorerklæring ikke kan opfylde persondatalovens krav om opfølgning, da erklæringen ikke har til formål at kontrollere, om persondataloven overholdes.

Ministeriet skal hertil bemærke, at Sundhedsstyrelsen har noteret sig Rigsrevisionens kritik.

Det kan supplerende bemærkes, at Sundhedsstyrelsens it-driftsleverandør (databehandleren) årligt får udarbejdet en ISAE 3000-erklæring af en uafhængig revisor om leverandørens overholdelse af persondataloven. Erklæringen er offentligt tilgængelig på leverandørens hjemmeside. Herudover følger Sundhedsstyrelsen op på databehandleraftalen ved månedlige driftsrapporteringer fra databehandleren, hvori sikkerhed indgår, audits på udvalgte områder samt som led i den normale daglige drift.

Det har således været Sundhedsstyrelsens vurdering, at databehandlerens sikkerhedsforanstaltninger er fuldt tilstrækkelige.

Institutionens eget tilsyn med sikkerhedsforanstaltninger
Det fremgår af beretningen:

- At Sundhedsstyrelsen ikke har retningslinjer for eget tilsyn med sikkerhedsforanstaltninger.
- At Sundhedsstyrelsen har udført kontrol af udvalgte punkter i sikkerhedsbekendtgørelsen.

Ministeriet kan hertil oplyse, at retningslinjer for Sundhedsstyrelsens eget tilsyn med de fastsatte sikkerhedsforanstaltninger vil blive udarbejdet inden 1. marts 2015.

Ad beretningens punkt 2.2: Institutionernes beskyttelse af fortrolige oplysninger om virksomheder
Opdaterede retningslinjer
Det fremgår af beretningen:

- At Sundhedsstyrelsen ikke har opdaterede retningslinjer for beskyttelse af fortrolige oplysninger om virksomheder (idet retningslinjerne ikke var blevet opdateret inden for det seneste år).

Sundhedsstyrelsen har noteret sig Rigsrevisionens kritik og indfører pr. 1. marts 2015 en praksis, hvorefter retningslinjerne bliver opdateret mindst én gang om året.

Brugeradgange
Det fremgår videre af beretningen:

- At Sundhedsstyrelsen følger en procedure for oprettelse af brugere, som sikrer, at alene de brugere, som har et arbejdsbetinget behov, får adgang til fortrolige virksomheds-oplysninger i systemet.
- At Sundhedsstyrelsen ikke gennemgår brugernes rettigheder med et passende interval.

Ministeriet kan oplyse, at Sundhedsstyrelsen har igangsat et arbejde med ændring af procedurer, således at kontrollen af brugeradgange fra og med 1. marts 2015 foretages mindst to gange om året, jf. sidste afsnit under punktet om brugeradgange og kontrol heraf, side 2.

Risikovurdering
Det fremgår af beretningen:

- At Sundhedsstyrelsen ikke har en opdateret risikovurdering for det undersøgte system (KAT).

Ministeriet skal hertil bemærke, at Sundhedsstyrelsen i oktober måned 2014 afsluttede en risikovurdering af systemet.

Der er samtidig sendt et eksemplar af ministerredegørelsen til Rigsrevisor, St. Kongensgade 45, 4. sal, 1264 København K.

Med venlig hilsen

Nick Hækkerup