Risk- och sårbarhetsanalys för Asthma Tuner

Region Jönköpings län

Steg i analysen

1. Beskrivning av molntjänsten - vad är det, vad används den till?
2. Bedömning av informationens känslighet – vilken typ av information lagras och/eller hanteras i den aktuella molntjänsten? Hur känslig är den?
3. Vilka system/tjänster/funktioner kommunicerar med och/eller är beroende av den aktuella molntjänsten?
4. Vilka risker uppstår när vi använder den aktuella molntjänsten?
5. Vilka risker uppstår om vi inte använder den aktuella molntjänsten?
6. Vilka åtgärdsförslag kan minska de identifierade riskerna om vi väljer den aktuella molntjänsten?
7. Vilka åtgärdsförslag kan minska de identifierade riskerna om vi inte väljer den aktuella molntjänsten?

1. Beskrivning av molntjänsten

Beskriv tjänsten övergripande i ett antal korta punkter, t.ex.:

- ***Vilket är användningsområdet?***

AsthmaTuner är ett behandling och egenvårdssystem för respiratoriska sjukdomar. AsthmaTuner kan förbättra astmakontrollen genom att erbjuda information och behandlingsrekommendationer som genereras baserat på patientens lungfunktion, symptom och vårdgivarförskriven behandlingsplan. AsthmaTuner möjliggör även egenvård av respiratoriska sjukdomar med hjälp av hantering av lungfunktion och användarrapporterad data och genom att erbjuda information.

Systemet består av: Careportal – Vårdgivargränsitt – Web app som nås via webbläasare, AsthmaTuner app – mobil app för patienter- Android och iOS, AsthmaTuner backend och API för lagring och transport av data mellan Careportal och appar – Compliant Cloud molntjänst från Cleura (https://cleura.com/sv/compliant-by-cleura/).

- ***Hur många ska använda den?***

Just nu 1500 patienter i piloten. 10% av befolkningen har astma som kan ta del av lösningen i framtiden.

7-8 vårdcentraler med ca 15 astmasköterskor.

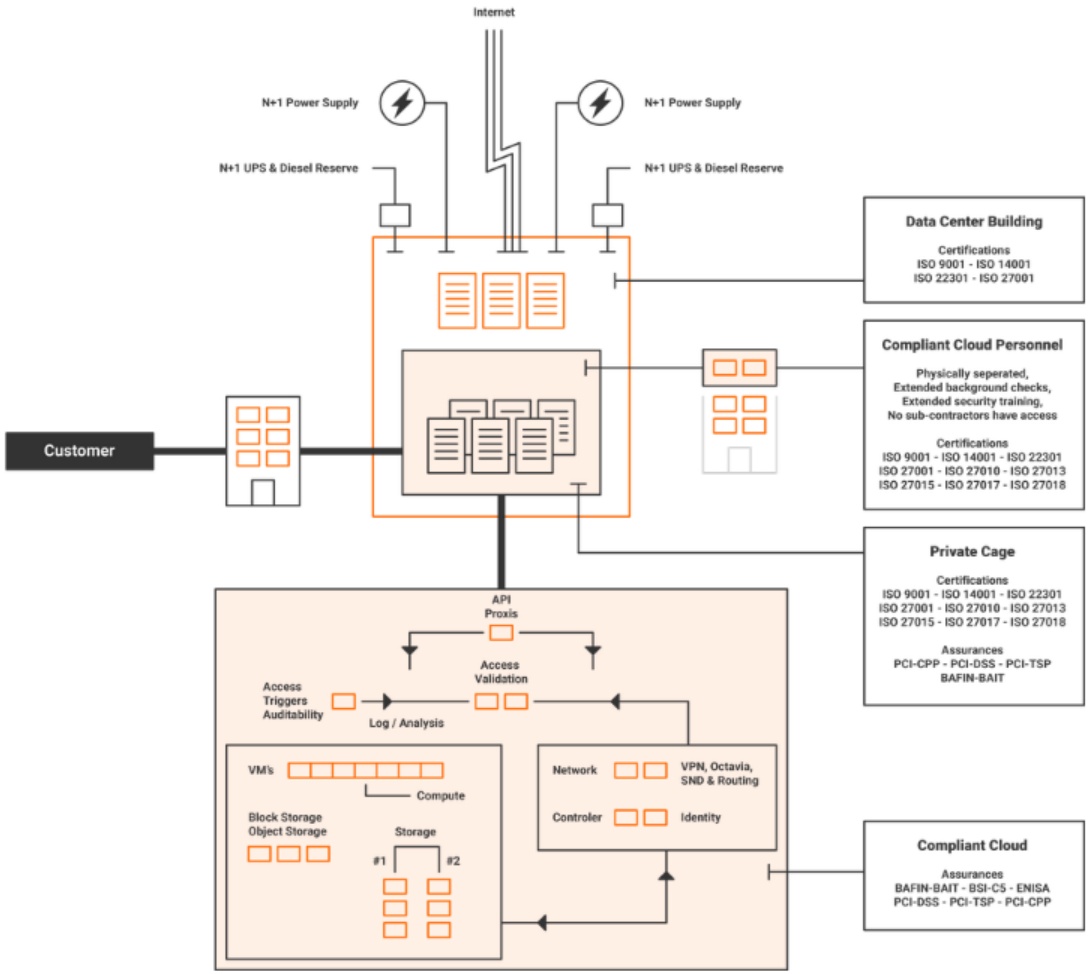
- ***Vem är leverantören?***

MediTuner AB (Svensk)

- ***Vad vet vi om leverantören?***

MediTuner är ett svenskt bolag och lagring sker på Compliant Cloud molntjänst från Cleura (lagring på svensk server i Sverige)

Compliant Cloud setup



Region Jönköpings län

2. Bedömning av informationens känslighet

- *Vilken typ av information lagras och/eller hanteras i molntjänsten? Hur känslig är den?*
- *Bedömning ska vara gjord utifrån de tre perspektiven – konfidentialitet, riktighet och tillgänglighet*
- *Utgångspunkten bör vara Klassas beskrivningar av informationssäkerhetsrisk: https://klassa-info.skl.se/demo/impactassesment*
- *Som stöd kan tabellerna på kommande sidor användas.*

Informationsmängd	Beskrivning/ kommentar	Nivå Konfidentialitet	Nivå Riktighet	Nivå Tillgänglighet
		0-4	0-4	0-4
Hälsodata (Lungfunktionsvärden, astmastatus, behandlingsplan etc.)	Från infoklassning 2020-09-22	1	0	1

3. Vilka system/tjänster/funktioner kommunicerar med och/eller är beroende av molntjänsten?

- AsthmaTuner är ett stand alone system som idag inte har några hårda integrationer och beroenden till andra externa tjänster.
- AsthmaTuner tjänst är beroende av Compliant Cloud från Cleura för lagring och transport av data. (Svensk server i Sverige)

4. Vilka risker uppstår när vi använder den aktuella molntjänsten?

Risker ur ett informationssäkerhetsperspektiv och ur ett rättsligt perspektiv (OSL och GDPR)

Gör en sida per risk!

Hotbild 1/Risk 1	***Skyddsvärd information röjs på grund av att känsliga personuppgifter förs över till molntjänst. Kan bryta mot GDPR artikel 9.3 och ge böter***				
Hotkälla	Sekretessbelagda uppgifter överförs till leverantör (Astma Tuner) och Compliant Cloud molntjänst från Cleura för lagring. Cleura och Asthma Tuner (MediTuner) bör omfattas av lagstadgad tystnadsplikt enligt lag				
Beskrivning av händelseförlopp	(Compliant Cloud molntjänst från Cleura) och Asthma Tuner (MediTuner) bör omfattas av lagstadgad tystnadsplikt enligt lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring av uppgifter och därmed uppfylls artikel 9.3 i GDPR.				
Beskrivning av konsekvenser	Kan finnas risk för sanktionsavgift om inte Cleura och Asthma Tuner (MediTuner) lyder under lagstadgad tystnadsplikt enligt lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring av uppgifter. Osäkert vad begreppen teknisk bearbetning och lagring innebär. Inte prövat av domstol ännu därmed osäkert rättsläge.				
	Bedömning av sannolikhet och konsekvens av hotet. Placeringen ger en indikation om vilken prioritet åtgärderna bör ges i åtgärdsplanen				
Konsekvens	Allvarlig				**Välj rätt ruta här!**
	Betydande				
	Måttlig				**1**
	Försumbar				
Sannolikhet		Mycket sällan	Sällan	Regelbundet	Ofta

Region Jönköpings län

Gör en sida per risk!

Hotbild 1/Risk 1	***Skyddsvärd information röjs på grund av att känsliga personuppgifter förs över till molntjänst. Kan bryta mot Offentlighets och sekretesslagen (OSL)***				
Hotkälla	Molntjänst				
Beskrivning av händelseförlopp	Sekretessbelagda personuppgifter (OSL) förs över till molntjänst. Rättsläget är osäkert kring vad röjande begreppet innebär.				
Beskrivning av konsekvenser	Den som röjer sekretesskyddade uppgifter på ett otillåtet sätt hålls personligt ansvarig och kan således bli föremål för straffsanktioner enligt 20 kap. 3 § Brottsbalken (BrB). Inte prövat av domstol ännu därmed osäkert rättsläge.				
	Bedömning av sannolikhet och konsekvens av hotet. Placeringen ger en indikation om vilken prioritet åtgärderna bör ges i åtgärdsplanen				
Konsekvens	Allvarlig				**Välj rätt ruta här!**
	Betydande				
	Måttlig				**2**
	Försumbar				
Sannolikhet		Mycket sällan	Sällan	Regelbundet	Ofta

Region Jönköpings län

Sammanfattning av risker som uppstår när vi använder den aktuella molntjänsten

Konsekvens	Allvarlig				
	Betydande				
	Måttlig				**1,2**
	Försumbar				
Sannolikhet		Mycket sällan	Sällan	Regelbundet	Ofta

Risk 1: Artikel 9.3 GDPR
Risk 2: Röjande enl. OSL
Risk 3: Namn
Risk 4: Namn
Risk 5: Namn

Region Jönköpings län

5. Vilka risker uppstår om vi inte använder den aktuella molntjänsten?

- Regionens patienter väljer bort RJL som vårdgivare om dem inte tillhandahåller tidsenliga standardverktyg
- Riskerar att stora patientgrupper får sämre behandlingsresultat
- Personalen får sämre arbetsmiljö när dom inte har koll på patienter
- Fler patienter söker akut pga dålig astmakontroll

Gör en sida per risk!

Hotbild 1/Risk 1	***Vikande patientunderlag***				
Hotkälla	Föråldrade system				
Beskrivning av händelseförlopp	Astmatuner och linanande tjänster är något som invånarna förväntar sig att möta. Möter vi inte förväntningarna väljer de andra tjänster.				
Beskrivning av konsekvenser	Regionens patienter väljer bort RJL som vårdgivare om dem inte tillhandahåller tidsenliga standardverktyg Det gör att vi tappar vårt ekonomiska underlag				
	Bedömning av sannolikhet och konsekvens av hotet. Placeringen ger en indikation om vilken prioritet åtgärderna bör ges i åtgärdsplanen				
Konsekvens	Allvarlig				
	Betydande				**1**
	Måttlig				
	Försumbar				
Sannolikhet		Mycket sällan	Sällan	Regelbundet	Ofta

Region Jönköpings län

Gör en sida per risk!

Hotbild 2/Risk 2	***Sämre behandlingsresultat***				
Hotkälla	Vi når färre patienter och har sämre verktyg				
Beskrivning av händelseförlopp	Vi har inte tid att kalla alla patienter för kontroll och patienter som inte har akuta problem söker sällan vård för sin astma. När det inte är på patienternas villkor kan denna grupp välja bort kontroller.				
Beskrivning av konsekvenser	Fler patienter har sämre funktion i sin vardag, får sämre lungfunktion över tid.				
	Bedömning av sannolikhet och konsekvens av hotet. Placeringen ger en indikation om vilken prioritet åtgärderna bör ges i åtgärdsplanen				
Konsekvens	Allvarlig				
	Betydande				**2**
	Måttlig				
	Försumbar				
Sannolikhet		Mycket sällan	Sällan	Regelbundet	Ofta

Region Jönköpings län

Gör en sida per risk!

Hotbild 3/Risk 3	***Sämre arbetsmiljö***				
Hotkälla	Bristande översikt över sin arbetssituation				
Beskrivning av händelseförlopp	Idag finns det ingen astmamottagning som är bemannad för att kalla alla sina astmapatienter på det sätt som är föreskrivet. Med Astmatuner så har de en möjlighet att ha koll på alla sina patienter och vet vilka som är dåliga/behöver åtgärdas.				
Beskrivning av konsekvenser	Personalen får sämre arbetsmiljö när dom inte har koll på patienter. KÁSAM				
	Bedömning av sannolikhet och konsekvens av hotet. Placeringen ger en indikation om vilken prioritet åtgärderna bör ges i åtgärdsplanen				
Konsekvens	Allvarlig				
	Betydande				**3**
	Måttlig				
	Försumbar				
Sannolikhet		Mycket sällan	Sällan	Regelbundet	Ofta

Region Jönköpings län

Gör en sida per risk!

Hotbild 4/Risk 4	Fler akutbesök				
Hotkälla	Sämre behandlade patienter leder till fler akuta besök				
Beskrivning av händelseförlopp	Astmatuner leder både till bättre underhållsbehandling OCH kan upptäcka en försämring innan man själv märker av det och då kan man behandla tidigare och undvika potentiella besök.				
Beskrivning av konsekvenser	Flera oplanerade (onödiga)akuta besök				
	Bedömning av sannolikhet och konsekvens av hotet. Placeringen ger en indikation om vilken prioritet åtgärderna bör ges i åtgärdsplanen				
Konsekvens	Allvarlig				
	Betydande			**4**	
	Måttlig				
	Försumbar				
Sannolikhet		Mycket sällan	Sällan	Regelbundet	Ofta

Region Jönköpings län

Sammanfattning av risker som uppstår om vi inte använder den aktuella molntjänsten

Konsekvens	Allvarlig				
	Betydande			4	**1,2,3**
	Måttlig				
	Försumbar				
Sannolikhet		Mycket sällan	Sällan	Regelbundet	Ofta

Risk 1: Vikande patientunderlag
Risk 2: Sämre behandlingsresultat
Risk 3: Sämre arbetsmiljö
Risk 4: Fler akuta besök

Region Jönköpings län

6. Vilka åtgärdsförslag kan minska de identifierade riskerna om vi använder den aktuella molntjänsten?

Hotbild	Risk-bedömning	Åtgärd	Prioritet	Ansvarig

Region Jönköpings län

6. Vilka åtgärdsförslag kan minska de identifierade riskerna om vi inte använder den aktuella molntjänsten?

Hotbild	Risk-bedömning	Åtgärd	Prioritet	Ansvarig

Region Jönköpings län

Utlåtande juridik och infosäk

Asthma Tuner har bytt lagringsplattform från Microsoft Azure (amerikanskt) till Compliant Cloud molntjänst från Cleura som är svensk och där lagring fysiskt sker i Sverige. Leverantören till Asthma Tuner heter MediTuner AB som också är svenskt.

1 jan 2020 kom en ny lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning och lagring av uppgifter. Den aktuella lagen innebär att en tjänsteleverantör och dess underleverantör som utför endast teknisk bearbetning eller lagring åt en myndighet är underställd straffsanktionerad tystnadsplikt. Därmed borde art 9.3 GDPR inte vara ett juridiskt hinder mot att molntjänstföretaget behandlar uppgifterna om de endast utför teknisk bearbetning eller lagring.

Rättsläget är osäkert om vi anses röja sekretessbelagda uppgifter när vi för över dessa till en molntjänst

För djupare analys se bifogat material

Rekommendation

Astmatuner är den första hemmonitoreringsprodukten som är så pass bra att den uppskattas och sprids till patienter och personal utan att behöva lägga kraft för att sprida den. Den är den första av de produkter som vi hoppas kommer revolutionera sjukvården får våra kroniskt sjuka patienter. Att sluta använda den skulle vara ett kraftfullt bakslag för länets astmavård.

Servrarna ligger på svensk mark, med svenskt ägande och uppfyller alla kända säkerhetsnormer.