Molntjänster från Microsoft – En checklista för vårdorganisationer i Sverige

Att börja använda molntjänster inom sjukvården är inte längre en fråga *om*, utan frågan är snarare *när*. Men vilken molnlösning ska man välja?

Microsoft har sammanställt en checklista med sjukvårdsspecifika krav samt en allmän checklista för molnanskaffning. Den här checklistan är till för att hjälpa dig i ditt val av molntjänster för din vårdorganisation men utgör inte juridiska råd. För att garantera att det lokala regelverket uppfylls bör du alltid söka oberoende juridisk rådgivning.

Du kommer att se att Microsofts molnlösningar är:

- ✓ Designade för att möta vårdorganisationers behov av patientcentrerad samverkan, robust säkerhet och efterlevnad av lokala bestämmelser kring integritet och hälsoinformation, såsom den svenska personuppgiftslagen (PUL), den svenska apoteksdatalagen, den svenska patientdatalagen och Socialstyrelsens föreskrifter (SOSFS).

- ✓ Skapade för att ge den användarvänlighet och produktivitet som krävs i vården för affärskritiska applikationer samtidigt som de ger beslutsfattare flexibilitet och valfrihet.

Microsoft vill vara din pålitliga molnpartner och vi är stolta över att just Microsofts HealthVault är den plattform som valdes för svenska medborgares hälsokonton av Apotekens Service AB 2013.

Checklista för köp av molntjänst

Checklista	Frågor att ställa	Microsofts svar
✓ Moln på dina villkor	✓ Erbjuder molnleverantören flexibilitet och valmöjligheter vad gäller lösningar för produktivitet och samarbete?	✓ Microsofts produktivitetsplattform består av ett antal olika tjänster och paket som kan installeras på plats, användas över nätet eller en kombination av båda. En flexibilitet som är oerhört värdefull när din verksamhet förändras eller växer. ✓ Office 365 har erbjudanden med rätt funktioner till rätt pris för sjukvårdsanställda som hittills haft lite eller ingen tillgång till innehålls- och meddelandefunktioner, t.ex. sköterskor, deltidsanställda eller inhyrd personal. ✓ Oavsett vad du har för behov och oavsett vad dina partner har för IT-kapacitet så kan Microsoft underlätta en övergång till molnet på dina villkor, med den säkerhet och flexibilitet du behöver. Det här gäller även om du ska integrera en nyförvärvad organisation med gammalmodiga produktivitetsverktyg eller integrera privatmottagningar som använder regelstridiga molntjänster. ✓ Vårdorganisationer jobbar ofta med ansträngd budget. Microsoft ger dig alternativet att välja de molnerbjudanden du behöver nu och betala enligt en abonnemangsmodell.
✓ Storföretags-anpassad	✓ Har molnleverantören erfarenhet av stora företag och myndigheter inom sjukvårdssektorn?	✓ Microsoft har i över 20 år försett sjukvårdsorganisationer med storföretagsanpassade produktivitetslösningar som förenklat kommunikation och informationsinhämtning.
	✓ Erbjuder de lösningar för sina storföretagskunder som skiljer sig från vad privatkunder får?	✓ Office 365 är molnversionen av de lika välkända och kraftfulla och redan storföretagstestade Microsoft Exchange, SharePoint, Lync och Office Professional Plus. ✓ Microsofts Enterprise-molnstjänster hålls logiskt åtskilja från privatkunders onlinetjänster.
	✓ Kan jag få användning för mina nuvarande investeringar i programvara och utbildning?	✓ I Office 365 kan du dra nytta av att vara bekant med tidigare Microsoft-produkter för att övergången till molnet ska gå smidigare, utan brant inlärningskurva för användarna. ✓ Du kan lägga till Office 365 till ditt nuvarande företagsavtal, så att du kan flytta till molnet och samtidigt få användning för nuvarande Microsoft-investeringar.
	✓ Går det att märka information som sekretessbelagd?	✓ Microsoft Office och Office 365 låter dig behålla det ursprungliga dokumentformatet, vattenstämplar och signaturer över alla enheter och platser. Din personal slipper den frustration som det innebär att förlora sådant när man använder molntjänster riktade till konsumenter.
	✓ Kommer affärskritiska data och tjänster vara tillgängliga och stödjas dygnet runt?	✓ Office 365 erbjuder ett finansiellt uppbackat servicenivåavtal (SLA) med 99.9 % upptid, och telefonsupport dygnet runt.
	✓ Vad händer om något går fel?	

Checklista svenskt regelverk

Område	Källa	Scenario	Krav	Microsofts position
Säkerhet och åtkomstkontroll	Apoteks- och patientdatalagen och SOSFS	Apoteks- och vårdgivare	Informationen måste lagras på ett sätt som skyddar den från obehörig åtkomst.	***Säkerhet*** • Microsoft organisation, Global Foundation Services (GFS), ansvarar för att tillhandahålla datacenter och fysisk infrastruktur för Office 365 som molntjänst. Dess säkerhetsprocesser granskas regelbundet av externa revisorer. • GFS har fått certifieringarna ISO 27001 och EU Safe Harbor och har klarat SSAE 16 SOC2 Type II. • Office 365 uppfyller många internationella branschstandarder, som ISO/IEC 27001:2005, PCI, SSEA16 SOC1 Type II, EUs Standardkontraktsklausuler och FISMA. • Microsofts fysiska säkerhetsåtgärder innefattar: (i) strikt åtkomstkontroll, (ii) biometrisk avläsning, (iii) videoövervakning, (iv) redundant strömförsörjning från olika leverantörer, (v) extra batterier och dieselgeneratorer, (vi) klimatkontroll, (vii) brandskydd och -släckning. • Microsofts säkerhetsåtgärder för data och nätverk innefattar: (i) säkerhetsbevakning, (ii) hot- och sårbarhetshantering, (iii) åtkomstkontroll, fil-/dataintegritet, (iv) två-faktors autentisering, (v) intrångsdetektering, (vi) malwareskydd (vii) edge-routrar och brandväggar • Microsoft har 49 olika FIPS 140-2- certifikat för sina krypteringsfunktioner: Azure Trust Services krypterar data i vila; Forefront Protection for Exchange skyddar data i rörelse. • QualysGuard (söker sårbarheter) verifierar statusen på säkerhetsuppdateringar.
			Användaren måste implementera åtkomstkontroller som verifierar användarens identitet på två olika sätt (d.v.s. två-faktors autentisering), enligt Socialstyrelsens riktlinjer.	***Kontroll*** • Windows Azure Active Directory erbjuder två-faktors-autentisering. • Utvecklare kan använda identifiering och autentisering på applikationsnivå via Windows Identity Foundation. • Microsoft erbjuder också (i) Active Directory Federation Services 2.0 (en säkerhetsnyckeltjänst), och (ii) Windows Azure Access Control Services. • Active Directory Organisational Units kontrollerar och förhindrar obehörigt och oavsiktligt informationsutbyte via delade systemresurser.

Checklista svenskt regelverk

Område	Källa	Scenario	Krav	Microsofts position
Integritet – kontroll över dina egen data	Apoteks- och patientdatalagen	Apoteks- och vårdgivare	Åtkomstkontroll måste implementeras men det finns inga specifika krav på hur den ska utformas.	***Integritet*** • Det är dina data. Du har kontinuerlig tillgång, du styr vem som har tillgång och vad de har för rättigheter. Du kan när som helst ta bort dina data från molnet utan att behöva underrätta Microsoft i förväg. • Datalagring och -behandling är logiskt separerad mellan olika användare av samma tjänst med hjälp av strukturen och funktionerna i Active Directory® som utvecklats specifikt för att bygga, hantera och säkra miljöer för flera användare. Multitenant- arkitekturen garanterar att kunddata som lagras i delade Office 365-datacenter inte kan tillgås av någon annan organisation. Organizational Units (OUs) i Active Directory kontrollerar och förhindrar otillåtna och oavsiktliga informations-överföringar via delade systemresurser. Användarna isoleras från varandra baserat på säkerhetsgränser ("silos") logiskt separerade av Active Directory. Dedikerad arkitektur för endast en användare finns också att välja.
			Datatillgången måste kontrolleras regelbundet och systematiskt; loggar på läsnivå krävs.	• QualysGuard granskar användarnas tillgång till system och databaser. • Windows Azure Diagnostics gör det möjligt att samla in omfattande diagnostiska uppgifter för att stödja felsökning av en tjänst. Den stödjer ett antal diagnostikfunktioner (t.ex. Windows Azure-loggar, Windows Event -loggar, IIS-loggar) • I SQL Azure hanteras transaktionsloggningen automatiskt av SQL Azures infrastruktur: SQL Server Analytics and Reporting Services står till förfogande. SQL Azure Reporting är en molnbaserad rapporteringstjänst som bygger på SQL Azure Database, SQL Server och SQL Server Reporting Services-tekniken
			Loggar måste sparas i 10 år och den behöriga användaren måste, innan åtkomst, ta beslut om huruvida han eller hon har behörighet att tillgå viss information. Alla förändringar av en patientjournal måste loggas.	• Se informationen ovan om tillgång och loggar.
			Informationen måste lagras på ett sätt som överensstämmer med den svenska personuppgiftslagen, d.v.s. aktuell och korrekt data.	• Microsoft respekterar din integritet; vi behandlar bara din information i den mån det krävs för att leverera den tjänst som du har begärt. ○ Vi analyserar inte dina data för att rikta marknadsföring mot dig och ser den inte heller som en produkt att sälja vidare till andra. ○ Vi använder inte dina data för att förbättra våra analyser.

Checklista svenskt regelverk

Område	Källa	Scenario	Krav	Microsofts position
Integritet - kontroll över dina egen data	Apoteksdatalagen	Apotek	Informationsförfrågningar ska begränsas och stå i relation till receptet, enligt vad som anges i apoteksdatalagen.	• Vi behandlar bara dina data i den mån det krävs för att leverera den tjänst som du har begärt, Microsoft analyserar inte dina data för att rikta marknadsföring mot dig för att förbättra våra analyser. • Microsofts företagsmoln hålls logiskt avskilt från privatpersoners tjänster. • Microsoft erbjuder möjligheten att lägga till automatiserad policybaserad mejlkryptering i Office 365 genom Microsoft ForeFront Protection for Exchange och Microsoft Exchange Hosted Encryption.
			Information måste raderas när den inte längre behövs för de godkända syften som anges i apoteksdatalagen. Informationen måste antingen permanent anonymiseras eller raderas på ett sådant sätt att den inte kan återskapas i efterhand.	• Kunder kan när som helst ta bort data från molnet utan att behöva underrätta Microsoft i förväg.
	Patientdatalagen	Vårdgivare	Information som är del av en patientjournal får bara raderas om: ○ Patienten begär det, och/eller andra personer vars information är registrerad i journalen; ○ Begäran har godkänts av Socialstyrelsen ○ Det finns god anledning att radera informationen; ○ Det är uppenbart att informationen inte behövs för vården av patienten; och ○ Det finns inga andra anledningar att behålla informationen ur ett samhälleligt perspektiv. Registeransvarig bär ansvaret för att skyldigheterna uppfylls (men kan förstås delegera till någon annan att uppfylla kravet). Alla borttagningar måste antecknas (bl.a. information om vem som tagit bort uppgiften och när den togs bort).	• Kunder kan när som helst ta bort data från molnet utan att behöva underrätta Microsoft i förväg. • Microsoft använder bästa arbetssätt för borttagning av data och en rensningslösning som uppfyller NIST 800- 88.

Checklista svenskt regelverk

Område	Källa	Scenario	Krav	Microsofts position
Rättning	Patient-datalagen	Vårdgivare	Det måste finnas rutiner för att rätta, bevara, blockera och sortera personlig information. Det finns inga mer specifika instruktioner vad gäller de här kraven. Den registeransvarige har ansvar för att kraven uppfylls (men kan förstås delegera uppgiften till någon annan).	• Inbyggda funktioner hjälper kunder att möta de här skyldigheterna. • Med Office 365:s eDiscovery Center kan kunderna bevara och hitta information över hela sin organisation. Regelansvariga kan identifiera, hålla och analysera organisationens data från Exchange Online, SharePoint Online och Lync Online. • Känslig information kan skyddas med Data Loss Prevention (DLP)-funktionen i Office 365. • Exchange Online erbjuder inbyggd DLP som kan sträckas för att stödja policyer som är viktiga för din verksamhet
Organisering	Patient-datalagen	Vårdgivare	All informationsbehandling måste uppfylla krav på patientsäkerhet, god kvalitet och kostnadseffektivitet. Det finns inga mer specifika instruktioner gällande de här kraven.	• Office 365 är själv kompatibelt med många internationella branschstandarder, t.ex. ISO/IEC 27001:2005, PCI, SSEA16 SOC1 Type II, EU Model Clauses och FISMA. Vi ordnar externa granskningar och certifieringar så att du kan lita på att våra tjänster är korrekt designade och drivs med rigorösa säkerhetsåtgärder.
Klassificering	Sekretess-lagen	Vårdgivare	Information måste stämplas som konfidentiell. Det är upp till kunden att avgöra vilken information som ska hemligstämplas.	• Office 365 låter användarna behålla det ursprungliga dokumentformatet, vattenstämplar och signaturer över alla olika enheter och platser. • Microsoft klassificerar information efter hur mycket den kan påverka verksamheten, och användare kan använda Microsofts metod för att klassificera sin information. • Microsoft Online Services-standarderna ger vägledning för att klassificera materialet i olika säkerhetsklasser, och implementerar sedan en standarduppsättning av säkerhets- och integritetsattribut.
Språk	Patient-datalagen	Vårdgivare	Hälsoinformation ska generellt sett vara på svenska.	• Du kan själv ställa in visningsspråk för Office 365, Lync Online och SharePoint Online - alla på en gång.