Safety first! Digitalisering av kommunikation inom vården

GENERIC • WHITE PAPER

“År 2025 ska Sverige vara bäst i världen på att använda digitaliseringens och e-hälsans möjligheter i syfte att underlätta för människor att uppnå en god och jämlik hälsa och välfärd samt utveckla och stärka egna resurser för ökad självständighet och delaktighet i samhällslivet.”

VISION E-HÄLSA 2025

Med Vision e-hälsa 2025 tar regeringen och Sveriges kommuner och regioner (SKR) ett grepp om digitalisering inom vården. Utvecklingen går snabbt, inte minst efter att Covid 19-pandemin skyndat på behovet av digitala möten och flöden.

Vinsterna med digitalisering är stora för såväl vårdgivare som vårdtagare. Mer resurser kan läggas på att möta och ta hand om patienter om föråldrade och ineffektiva administrationssystem och kommunikationsvägar som fax och telefon kan ersättas med samtida, digitala och mobila tjänster.

Uteblivna besök kostar miljarder

Redan 2018 räknade Västra Götalandsregionen ut att kostnaden för uteblivna besök uppgick till en halv miljard[1]. Om motsvarande gäller för andra regioner, dvs att 6 procent av vårdbesöken uteblir utan av- eller ombokning, lär kostnaden uppgå till flera miljarder sammanlagt för landets 21 regioner.

2018 räknade Västra Götalandsregionen ut att kostnaden för uteblivna besök uppgick till en halv miljard.

Det är en kostnad som skulle minska drastiskt med automatiserade lösningar för besökspåminnelser, stöd för av- och ombokning och möjligheter att boka sig med kort varsel på andras avbokade tider – vilket också Västra Götalandsregionen erfarit då en del mottagningar infört sådana tjänster.

Omställning på ett säkert sätt

Vision e-hälsa strävar efter en mer effektiv och jämlik vård med ökade möjligheter till informationsutbyte mellan exempelvis hälso- och sjukvård och socialtjänst. Denna transformation måste ske med säkerhet i första hand då informationen i hög grad består av känsliga personuppgifter[2] som måste skyddas enligt världens strängaste regelverk för persondataskydd; GDPR[3] samt den kompletterande Patientdatalagen[4]. Dessa lagar, och en mängd andra, gäller såväl offentliga som privata vårdgivare. Det innebär, som vi kommer att se, att de publika molntjänsternas ägarförhållanden får stor betydelse.

Ökad tillgänglighet och verksamhetsnytta

Digitalisering är i hög grad utveckling av applikationer och processer som förenklar människors vardag. Sömlösa användarupplevelser oberoende av plattform med utbyten och analyser av stora mängder information kännetecknar dem. Innovationskraften är stor och dessa applikationer är i princip omöjliga att genomföra användarvänligt och kostnadseffektivt utan publika molntjänster. Inom såväl offentlig som privat verksamhet har applikationer i molnet redan i många fall lett till ökad tillgänglighet och verksamhetsnytta med god teknisk säkerhet till rimliga kostnader.

Ogiltigförklaringen av The Privacy Shield

Informationen kan också vara eftertraktad, inte minst av stater som vill ha insyn och som ibland stiftar lagar som ger dem rätt att under vissa omständigheter begära uppgifter direkt från molntjänstleverantören. Det mest kända exemplet är USA som med The CLOUD Act (Clarifying Lawful Overseas Use of Data Act) ger amerikanska myndigheter möjlighet att begära att bl.a. leverantörer av elektroniska kommunikationstjänster och molntjänster bevarar eller lämnar ut den data som där hanteras. Indien, Kina och Ryssland är andra exempel på länder med liknande lagstiftningar som USA.

Fram till sommaren 2020 skyddades överföringen av personuppgifter mellan USA och Europa med regelverket The Privacy Shield som ett sätt uppfylla kraven för persondataskydd enligt GDPR. Men i juli 2020 ogiltigförklarades[5] regelverket av EU-domstolen i det s.k. Schrems II-målet[6].

Vad innebär ogiltigförklaringen av The Privacy Shield och vilka konsekvenser får det?

För att digitala tjänster ska fungera utan avbrott flyttas information mellan servrar där det för närvarande finns kapacitet. Marknaden för publika molntjänster domineras av några få, gigantiska amerikanska aktörer vilket innebär att finns det data som amerikanska myndigheter av någon anledning vill ha tillgång till är tjänsteleverantören skyldig att lämna ut dessa enligt CLOUD Act.

Att EU-domstolen ogiltigförklarade The Privacy Shield med omedelbar verkan får i det närmaste oöverskådliga konsekvenser för bland annat handeln mellan EU-länder och USA. Ipraktiken innebär det att överföring av personuppgifter till USA är ett brott mot GDPR.

I praktiken innebär det att överföring av personuppgifter till USA är ett brott mot GDPR.

Hävandet av The Privacy Shield blev en skräll för organisationer som hanterar data som inte ens omfattas av samma sekretess som exempelvis journaluppgifter. Men redan 2018 fastslog eSam, ett samverkansprogram mellan 27 myndigheter och SKR för att ta tillvara digitaliseringens möjligheter, att sekretessbelagda uppgifter anses röjda[7] om tjänsteleverantören kan bli skyldig att lämna ut dem som en följd av regler i ett annat land:

> **"Om sekretessreglerade uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt, får uppgifterna anses vara röjda."**
>
> **ESAM 2018**

Konkret innebär det att sekretessbelagda personuppgifter som exempelvis journaluppgifter är röjda enbart genom att hanteras av en amerikansk molntjänst – eller en tjänst med ett ägarförhållande till USA eller till ett land med en lagstiftning som inte är enligt samma nivå som GDPR.

Utifrån EU-domstolens dom att häva the Privacy Shield har Dataskyddsmyndigheten uppdaterat sina rekommendationer[8] gällande organisationer med flöden av personuppgifter som kan komma att överföras till USA eller annat tredje land. EU-kommissionen antog i juni 2021 en ny uppsättning standardavtalsklausuler för överföring av personuppgifter till tredjeland som ska göra det lättare att följa Schrems II-domen[9]. Men räcker det inte som skydd att den amerikanska molntjänsten har sin serverhall i Eskilstuna eller Frankfurt och ett kontor registrerat i ett EU-land? Svaret är nej eftersom CLOUD Act ger amerikanska myndigheter rätt att begära att information lämnas ut från serverhallar varsomhelst i världen så länge leverantören av molntjänsten har samröre med USA, exempelvis är ett amerikanskägt bolag.

Varför är personskyddet avgörande vid val av leverantör av kommunikationstjänster inom vården?

Redan idag har en stor andel av Sveriges kommuner och regioner investerat i applikationer som erbjuds av den privata marknaden och driftas i publika molntjänster. Samtidigt identifierar SÄPO[10] teknikutvecklingen som ett hot mot Sverige. Utkontraktering av IT, där privata molntjänster ingår, ser SÄPO som en potentiell risk då leverantören hanterar olika kunders system och information i samma fysiska datorsystem. Om en stor mängd sekretessbelagd information hamnar hos en enskild leverantör finns risken att den blir ett attraktivt mål för underrättelsetjänster i andra länder, exempelvis med en agenda att skapa osäkerhet, öka polariseringen i samhället eller kränka enskildas integritet.

Hälso– och sjukvården lyder under en mängd regelverk vad gäller persondataskydd, sekretess och arkivering. Den klassas också av Myndigheten för samhällsskydd och Beredskap, MSB, som samhällsviktig. Störningar eller bortfall av verksamheten kan orsaka kriser som hotar samhället. Därför är det viktigt att utvecklingen av digitala tjänster med syfte att underlätta för vårdtagare och vårdgivare inte blir ett säkerhetshot.

Att säkerställa att trafik och lagring sker i ett svenskägt bolag och aldrig lämnar Sverige är ett sätt att garantera säkerheten.

Även om den publika molntjänsten med kopplingar till USA hanterar data i serverhallar inom EU så kan amerikanska myndigheter alltid komma åt den utan behöva begära tillstånd av de lokala myndigheterna.

Att säkerställa att trafik och lagring sker i ett svenskägt bolag och aldrig lämnar Sverige är ett sätt att garantera säkerheten.

Vilka viten riskerar man att få?

Företag som Microsoft, Google och Amazon har global närvaro och finns i nästan alla länder. För det måste de underkasta sig de aktuella ländernas lagstiftning. Om dessa lagar kräver att tjänsteleverantören lämnar ut persondata i hemlighet[11] till landets myndigheter så gör de det. Visselblåsaren Edward Snowden avslöjade den amerikanska statens omfattande övervakning av sina medborgare, Google har avslöjats gå den kinesiska regimens ärenden. Men som tjänsteleverantör har man följt de lagar som finns i landet: det amerikanska personskyddet är vida underlägset det europeiska och diktaturers maktutövning sker i hög grad genom övervakning av medborgarna. Om en europeisk medborgare misstänker att personinformation läckt till en främmande makt kan hon eller han anmäla överträdelsen enligt GDPR. Beroende på hur allvarlig överträdelsen är kan sanktionsavgiften för företag uppgå till 20 miljoner euro eller 4 procent av den globala årsomsättningen. I Sverige kan även myndigheter utkrävas sanktionsavgifter[12] på upp till tio miljoner kronor. Datainspektionen bedömer bland annat hur allvarlig överträdelsen är, hur stor skada som skett, om det är fråga om känsliga personuppgifter och om överträdelsen är avsiktlig.

Beroende på hur allvarlig överträdelsen är kan sanktionsavgiften för företag uppgå till 20 miljoner euro.

Hur tänka långsiktigt för att både få bra kommunikationstjänster och följa GDPR?

Digitalisering är en komplex verksamhet och handlar inte bara om IT utan om beteenden, processer och arbetssätt. En tjänst som inte är relevant, fungerar dåligt eller är svår att förstå kommer inte att användas. Effektiv informationshantering är grundläggande och innovationskraften finns inom det privata näringslivet. Vid val av leverantör finns det flera faktorer att ta hänsyn till. Hur hanteras datan och var lagras den? Hur bra är deras tjänster? Har de underleverantörer och har dessa i sin tur underleverantörer osv? Hur är de att samarbeta med?

5 saker du ska tänka på när du väljer samarbetspartner

Säkerheten ska alltid komma först, men det är också viktigt att undersöka innovationsförmåga, teknisk nivå och kapacitet då du väljer samarbetspartner eller leverantör av digitala kommunikationstjänster. Det är en ständigt pågående, iterativ process där tjänsterna måste hänga med i utvecklingen av människors behov och önskemål. En samarbetspartner ska ha förmågan att identifiera och lösa problem proaktivt.

1. Smarta lösningar

Att tjänsten är relevant och fungerar väl är grundläggande men inte alltid självklart i verkligheten. Säkerställ att leverantören är innovativ, kan sin sak och har den kapacitet som krävs för dina behov.

2. Stort tjänsteutbud

Det mesta har ännu inte hänt eller utvecklats. En samarbetspartner inom kommunikation måste kunna bevisa sin innovationskraft med konkreta erbjudanden. Områden som bör undersökas är:

- Har leverantören ett omfattande och skalbart utbud av tjänster för uppgiften som ska utföras?
- Är det en leverantör som framtidssäkrar dig för vad dina användare kommer att förvänta sig imorgon?

3. Enkla integrationer

Hur väl fungerar integrationen av tjänsten i det system ni använder eller kommer att använda? Den tekniska nivån måste vara väl utvecklad, dokumenterad och kunna bevisas.

4. Säker hantering och lagring av information

Slutsatsen av analysen av digitalisering inom vården är att publika molntjänster med utomeuropeiska ägarförhållanden inte kan garantera den personliga integriteten enligt GDPR. Leverantörer med enbart europeiskt ägarskap och egen drift är i nuläget de enda som uppfyller de regelverk som hälso- och sjukvården måste följa vad gäller persondataskydd, sekretess och arkivering.

5. Driftsäkerhet och support 24/7

Säker drift kräver en säker support. Frågor ni bör ställa er är:

- Vilken driftsäkerhet kan leverantören garantera?
- Vilken supportnivå erbjuds?
- Sker överföring av data till tredje part och finns då risk att sekretessbelagda personuppgifter är röjda?

En leverantör bör garantera mycket hög driftsäkerhet och erbjuda nationell support i egen regi dygnet runt, alla dagar i veckan

Undvik icke-svenska molntjänster om du vill vara helt säker på var patientdatan finns

Om du som är vårdgivare i Sverige vill vara helt säker på att följa de regelverk som du omfattas av vad gäller datahantering, oavsett om du verkar i en region, en kommun eller i ett privat vårdföretag, välj en svensk leverantör med egna serverhallar i Sverige. Kräv full insyn i ägarförhållanden och var datan finns fysiskt, "molnet" är som bekant bara en metafor för data som "flyter omkring" i olika serverhallar.

Du ska även ha koll på din leverantörs underleverantörer och om dessa i sin tur har underleverantörer etc.

Du ska även ha koll på din leverantörs underleverantörer och om dessa i sin tur har underleverantörer etc.

Försäkringskassan avvisar icke-svensk uppgiftshantering

2020 vann Generic en offentlig upphandling avseende ramavtal för SMS för Försäkringskassan[13]. Uppdraget består i att leverera meddelandetjänster med allra högsta krav avseende datalagring, säkerhet och personuppgiftsbehandling. Lösningen består bland annat av SMS-notifieringar via API och webbportal, e-identifiering och prenumerationstjänster.

I denna upphandling ställdes de hittills mest rigorösa och långtgående kraven på säkerhet och databehandling. Försäkringskassan har till exempel valt att inte godkänna aktörer som kan omfattas av CLOUD Act. Ramavtalet öppnar även för beställningar från andra myndigheter och är en tydlig indikation på vilken säkerhetsnivå som kommer att kravställas från svenska myndigheter framöver, något som alla aktörer inom hälso- och sjukvården kan se som ett rättesnöre.

I "Vitbok, Molntjänster i samhällsbärande verksamhet — risker, lämplighet och vägen framåt"[14] som Försäkringskassan publicerade i november 2019, alltså innan The Privacy Shield ogiltigförklarades av EU-domstolen, fastslår myndigheten:

"För att svenska myndigheter ska kunna fortsätta att dra fördel av digitaliseringens alla möjligheter bör vi därutöver — genom samverkan nationellt och inom EU — se till att de privata tjänster vi väljer att använda anpassas till våra behov och gällande lagstiftning samt har en säkerhetsnivå som gör att vi kan behålla kontrollen över vår verksamhet och information. På så vis kan vi dra fördel av den innovationskraft och effektivitet som ofta är förknippad med privata it-tjänster, samtidigt som vi säkerställer Sveriges intresse av digital suveränitet."

Kommunikationslösningar för hälso– och sjukvården med säkerheten främst

Säkerheten måste komma först när du väljer lösningar och leverantörer för digitaliserade kommunikationsflöden.

Säkerheten omfattar mer än persondataskydd. Utöver att regelverken ska följas krävs att tjänsten är användarvänlig, driftsäker, innovativ och effektiv.

Söker du en samarbetspartner med stor erfarenhet av säkra och effektiva kommunikationsflöden för en mängd användningsområden, kontakta oss. Vi har meddelandetjänster och kommunikationslösningar som effektiviserar bland annat bemanning och patientkommunikation, flöden för tidsbokning med påminnelser och möjligheter till om– och avbokning eller erbjudande om sista minuten–tider.

Alla dataflöden hanteras i våra säkerhetsklassade serverhallar i Sverige och vår support är i tjänst dygnet runt, årets alla dagar.

Alla dataflöden hanteras i våra säkerhetsklassade serverhallar i Sverige och vår support är i tjänst dygnet runt, årets alla dagar.

Säkrast på marknaden

Generic har en gedigen bakgrund inom säker kommunikation under extrema förhållanden. Idag är vi en högteknologisk aktör inom med–delanden för alla typer av användningsområden, utan att ha tappat kontakten med våra rötter.

Vi engagerar oss i dig

Du ska känna dig trygg med våra tjänster och kunna förvänta dig att vi ser till att allt fungerar som det ska, idag och i framtiden. Vi är 20 medarbetare i Luleå, Stockholm och Örebro som brinner för allt från personlig kundservice, heltäckande lösningar och teknisk utveckling.

Generic är noterat på OMX First North.

Kontakta oss

Tel: 020–31 00 41
SMS: 0730–12 12 01
E–post: kund@genericmobile.se
generic.se

Har du frågor kring gdpr/dpo maila oss på **datainf@genericmobile.se**

Slutnoter / Referenser

1) https://lakartidningen.se/aktuellt/nyheter/2019/01/farre-uteblivna-besok-med-sms-paminnelser-och-nya-arbetssatt/

2) https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter/

3) https://www.imy.se/verksamhet/dataskydd/

4) https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/vard/

5) https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/schrems-ii-domen-overforingar-till-tredje-land/

6) https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

7) https://www.esamverka.se/download/18.1d126bc174ad1e6c39cac3/1542007824143/eSam%20-%20Ra%C-C%88ttsligt%20uttalande%20om%20ro%CC%88jande%20och%20molntj%C3%A4nster.pdf

8) https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/overforing-till-tredje-land/schrems-ii-domen-overforingar-till-tredje-land/

9) https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

10) https://www.sakerhetspolisen.se/publikationer/om-sakerhetspolisen/sakerhetspolisen-2019.html

11) https://nextcloud.com/blog/us-cloud-companies-give-up-fight-for-privacy-of-their-users/

12) https://www.imy.se/om-oss/vart-uppdrag/sa-arbetar-vi-med-tillsyn/vad-kan-tillsynen-leda-till/

13) https://www.generic.se/nyheter_posts/generic-ny-leverantor-av-meddelandelosningar-till-forsakringskassan/

14) https://www.forsakringskassan.se/wps/wcm/connect/30cc57bd-b5cd-4e04-94cd-1f7a02a9ae1a/vitbok.pdf?MOD=AJPERES&CVID=&CACHE=NONE&CONTENTCACHE=NONE