
Fysioterapeuterna

Vårdens dataskydd efter GDPR

Stockholm den 12 december 2017

Martha Gurmu, Chefsjurist

- EU:s nya dataskyddsförordning (GDPR) träder i kraft 25 maj 2018.
- Samma datum upphävs personuppgiftslagen (PuL), som baseras på det gamla dataskyddsdirektivet.
- Någon motsvarighet till PuL kommer dock inte att införas, då tanken är att tillämpningen främst ska grundas direkt på förordningen.

- Vissa element av GDPR kommer dock att beskrivas i en kompletterande dataskyddslag.

- Dessa delar är dock inte mer gällande än övriga GDPR.

Hur blir det med vården när GDPR träder i kraft?

- För vårdens del finns separata dataskyddsregler i **patientdatalagen** (PDL).
- **PDL har företräde framför PuL, och kommer att fortsätta gälla efter GDPR.**
- För en sammanhållen bild av vårdens dataskyddsregler måste man därför titta på både PDL och GDPR.
- GDPR höjer den generella skyddsnivån för personuppgifter.

- PDL:s regler är dock strängare än PuL. **GDPR får därför mindre genomslag inom vården** än inom samhället generellt.
- **Sektorsspecifik reglering, t.ex. PDL, har företräde framför dataskyddslagen.**
- Den har dock en företräde framför GDPR.

På många, men inte samtliga, punkter resulterar GDPR alltså i att skyddsnivån för övriga samhället höjs till något som motsvarar PDL.

Behandlings begreppet

- Såväl GDPR som PDL reglerar ”behandling” av personuppgifter.

- Begreppets innebörd ändras inte genom GDPR.

- *”[Å]tgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.*

Minskad möjlighet att basera behandling på intresseavvägning

- Vid sidan av specifika regler om ändamål med personuppgiftsbehandling finns möjlighet att basera behandling på en avvägning av parternas intressen.

- Denna möjlighet minskar i GDPR.

  -För myndigheter avskaffas den helt.

Detta får dock liten relevans för hälso- och sjukvården, eftersom behandlingen där baseras på särreglerade ändamål.

Skyldighet att göra konsekvensbedömning

- Gäller för behandling som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.” (Art. 35 GDPR)
- Gäller dock **inte behandling** som **sker på basis av ”rättslig förpliktelse, allmänt intresse eller myndighetsutövning”.**

Enligt Socialdepartementets bedömning är hälso- och sjukvård både en rättsligt förpliktelse (landsting och arbetsgivare) och av allmänt intresse.

Denna skyldighet kommer därför som huvudregel inte bli aktuell för vårdgivare.

Personuppgiftsincidenter

”säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.”

För dessa gäller anmälningsplikt till Datainspektionen enligt GDPR.

- Anmälan ska ske **inom 72 timmar** från att incidenten upptäcks.
- I de fall där **uppgifter går förlorade** kan det finnas förutsättningar att göra avvikelse eller Lex Maria.
- Detta eftersom sämre tillgång till uppgifter om patienten påverkar patientsäkerheten.
- Allmänt gäller att anmälningsplikter inte utesluter varandra. Om förutsättningarna är uppfyllda är vårdgivaren ansvarig att göra flera anmälningar.

- Anmälan till Datainspektionen (DI) ska göras om det inte är osannolikt att incidenten leder till konsekvenser för fysiska personers rättigheter och friheter.

- Anmälan ska innehålla beskrivning av incidenten, sannolika konsekvenser och vilka åtgärder vårdgivaren avser vidta.

- Patienten ska underrättas om incidenten lett till ”hög risk för fysiska personers rättigheter eller skyldigheter”.

  – Undantag från detta gäller dock om den ansvariga har vidtagit åtgärder som innebär att risken sannolikt inte kommer att realiseras, om det skulle innebära en orimlig ansträngning, samt om t.ex. kryptering gör uppgifterna omöjliga att tyda för utomstående..

- DI kan i samband med anmälan fatta beslut om huruvida patienten ska underrättas eller ej.

- I dagsläget finns ingen uttrycklig skyldighet att informera patienten i dessa fall.

Förstärkt krav på information om behandling

- *Förstärkt krav på information om behandlings ska vara:*

  ”koncis, klar och tydlig, begriplig och lättillgänglig” (Art. 12.1.)

- Gäller t.ex. logglistor, där informationen idag ”ska vara utformad så att patienten kan bedöma om åtkomsten har varit befogad eller inte” (4:10 § HSLF-FS 2016:40).

Gäller även då samtycke inhämtas till olika slag av behandling, t.ex. till att ta del av journaler genom sammanhållen journalföring.

Utvidgad definition av känsliga personuppgifter

Känsliga uppgifter enligt PuL

13 § Det är förbjudet att behandla personuppgifter som avslöjar

a) ras eller etniskt ursprung,

b) politiska åsikter,

c) religiös eller filosofisk övertygelse, eller

d) medlemskap i fackförening.

Det är också förbjudet att behandla sådana personuppgifter som rör hälsa eller sexualliv.

Uppgifter av den art som anges i första och andra styckena betecknas i denna lag som känsliga personuppgifter.

- Definitionen utvidgas till att **även omfatta genetiska uppgifter, biometriska** uppgifter för att entydigt identifiera en fysisk person och uppgifter om sexuell läggning.
- Många av dessa punkter omfattas dock indirekt av den gamla definitionen (t.ex. är uppgifter om sexuell läggning i praktiken detsamma som uppgifter om sexualliv).
- Hälso- och sjukvården har genom PDL undantag från förbudet att behandla känsliga uppgifter.
- **Känsliga uppgifter undantaget hälsa får dock inte använda som sökbegrepp** (2:8 § PDL). Denna regel breddas till att omfatta genetiska/biometriska uppgifter och uppgifter om sexuell läggning.

Dataportabilitet

Enligt Art. 20 GDPR ska den personuppgiftsansvarige tillhandahålla registerutdrag i ett ”allmänt använt och maskinläsbart format i syfte att kunna överlämnas till en annan personuppgiftsansvarig”.

- Detta gäller dock bara om behandlingen baseras på samtycke eller avtal.

- **Skyldigheten gäller därför inte för hälso- och sjukvården.**

- Att skicka patientinformation via mail bryter dessutom mot de s.k. öppna nät-bestämmelserna.

”Rätten att bli bortglömd”

- Den registrerades rätt att få sina uppgifter raderade stärks betydligt i och med GDPR, vilket lyfts fram som en av de principiella nyheterna.

- Denna rätt kan dock begränsas av sektorsspecifik lagstiftning, och kommer så att göras av PDL.

- Patienter som vill få journaluppgifter utplånade måste alltså alltjämt ansöka om detta hos **IVO enligt 8:4 § PDL.**

Finalitetsprincipen

Sedan tidigare gäller att personuppgifter får behandlas för andra syften än de för vilka de samlats in, förutsatt att det nya syftet **”inte är oförenligt**” med det ursprungliga.

- Nytt i GDPR är dock att det nya syftet inte behöver ha någon separat rättslig grund.

- Den uppräkning av godkända syften som finns i PDL är alltså inte uttömmande.

- Det är viktigt att skilja frågan om vilka syften som är godkända överhuvudtaget, från de som är godkända för de specifika uppgifterna mot bakgrund av varför de samlats in.

- Bedömningen av huruvida ett nytt syfte är förenligt med det ursprungliga ska göras av den personuppgiftsansvarige, som ska beakta alla omständigheter, t.ex. i vilket sammanhang uppgifterna samlats in.

- Utrymmet är generellt sett mindre vid känsliga personuppgifter.

Sanktionsavgifter

- Möjligheterna att döma ut sanktionsavgifter ökar betydligt.
- Tak på ”20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.” (Art. 83.c.5 GDPR).

- Datainspektionen ansvarar för att påförandet av sanktionsavgifter ”i varje enskilt fall är effektivt, proportionellt och avskräckande.”…

Patientdatalagen

Inom vården behandlas känsliga personuppgifter i högre grad än i samhället i övrigt. Det är en nödvändighet för att verksamheten ska kunna fungera.

Samtidigt ställer det krav på att patientens och andras integritet accepteras. Generellt gäller att ju mer informationen vården har av patienter, desto bättre förutsättningar att ge god vård.

PDL försöker därför att balansera dessa två intressen mot varandra.

PDL styr behandling av personuppgifter inom hälso- och sjukvården.

– ”Behandling” definieras i PuL som *”Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.”*

- 1 kap. Allmänt
  - Definition av journalhandling
    - Även bilder och ljudfiler, t.ex. diktat, är journalhandlingar
    - ”Minnesanteckningar” är journalhandlingar
    - Även inkomna handlingar omfattas
  - PDL har företräde framför PuL
- 2 kap. Grundläggande bestämmelser
  - Samtyckesprincipen: behandling som inte tas upp i lagen får ske med samtycke
    - Dock ej inom sammanhållen journalföring
  - Den behandling som beskrivs i PDL får dock genomföras även om patienten motsätter sig den.

Definition

Definitionen av journalhandling:

”Framställning i skrift eller bild samt upptagning som kan läsas, ***avlyssnas*** *eller på annat sätt uppfattas endast med tekniskt hjälpmedel och som* ***upprättas eller inkommer*** *i samband med vården av en patient och som innehåller uppgifter om patientens hälsotillstånd eller andra personliga förhållanden eller om vidtagna eller planerade vårdåtgärder.”*

Ändamål med behandling

All behandling av personuppgifter måste relateras till något av dessa ändamål:

– 1. att [journalföra enligt PDL] och upprätta annan dokumentation som behövs i och för vården av patienter,

2. administration som rör patienter och som syftar till att ge vård i enskilda fall eller som annars föranleds av vård i enskilda fall,

3. att upprätta annan dokumentation som följer av lag, förordning eller annan författning,

4. att systematiskt och fortlöpande utveckla och säkra kvaliteten i verksamheten,

5. administration, planering, uppföljning, utvärdering och tillsyn av verksamheten, eller

6. att framställa statistik om hälso- och sjukvården.

- Uppgifter får bara finnas i journalen om de krävs för p.1-2.
  – När de sedan finns där får de dock användas för övriga ändamål i p. 3-6.

När ska man föra journal?

3 kap. 1 § PDL *Vid vård av patienter ska det föras patientjournal. […]*

Journalföring ska ske ”så snart som möjligt”.

- 48 timmar är tumregel enligt vägledande SoS-beslut.

Gränserna för journalföringsplikten framgår dock i praktiken indirekt av PDL och HSLF-FS 2016:40:s uppräkning av obligatoriska uppgifter att journalföra.

Signeringskravet

- Enligt **3:10 § PDL** ska en journalanteckning signeras av ”den som ansvarar för uppgiften” så länge inget synnerligt hinder finns mot det.”

- Det är därför viktigt att **enbart rätt person** signerar.

- ”Synnerligt hinder” är mycket sällsynt.

- Det krävs ”mycket starka skäl i det enskilda fallet”.

Om rätt person inte kan signera bör någon annan med rätt kompetens bedöma anteckningen.

  – Denna ska dock ej signera.

- Genom att signera intygar man att innehållet är korrekt.

- Vårdgivaren kan i sin informationssäkerhetspolicy besluta om undantag från signeringsplikten.

- Det ska då gälla anteckningar som inte rör genomförd vård, epikris eller väsentliga ställningstaganden.
  - Undantaget ska finnas inskrivet i informationssäkerhetspolicyn.

OBS: Socialstyrelsen har nyligen tagit bort den regel som indirekt ledde till att anteckningar skulle signeras inom 14 dagar.

- Signeringen har ingen betydelse för huruvida anteckningen är att anse som allmän handling (HFD 2013 ref. 33).

- Patient/närstående ska alltså kunna få ut även osignerade anteckningar.

- Samma princip borde gälla inom privat verksamhet.

- Många vårdgivare har valt att utesluta osignerade anteckningar vid patientens direktåtkomst via nätet. Detta är tillåtet eftersom det i grunden inte finns någon skyldighet att erbjuda patienten direktåtkomst överhuvudtaget. Detta ska dock framgå.

För vems skriver jag journal?

- Patienten har starka rättigheter knutna till journalen.

- Exempelvis att få läsa journalen, begära ut logglistor, få sin avvikande uppfattning antecknad och, indirekt genom sekretessreglerna, bestämma vilka andra som får läsa den.

OBS: patienten har inte rätt att styra innehållet i journalen.

- Innehållet styrs av lagstiftningen, som i sin tur anger ramar för vårdgivaren att avgöra vad som ska journalföras och inte.

Är journalen arbetsredskap eller informationskälla?

– Enligt 3:2 § PDL är journaler i första hand arbetsredskap.
  - I andra hand informationskälla för patient och andra

– 3:13 § PDL anger att texten ska vara så lätt som möjligt att förstå för patienten.
  - Samtidigt anger HSLF-FS 2016:40 att ett antal fackterminologiska publikationer ska användas.

I slutändan bör dock 3:2 § ha företräde framför 3:13 §

Språket i journaler ska vara svenska

- Undantag för norska och danska om den journalföringspliktiga har behörighetsbevis enligt, och engelska om personen har förordnande.
- Vårdgivaren ansvarar för noggrannhet och att ställningstaganden och genomförd vård finns även på svenska

– Bevaringstid 10 år efter att sista uppgiften fördes in.

Vad göra när man skrivit i fel patients journal?

- Tidigare krävdes ansökan om förstörande.

- Enligt ett principbeslut från IVO (nov 2013) kan dock texten numera flyttas till rätt patient utan ansökan om förstörande.

Patienter med skyddad identitet

Skyddad identitet finns i tre grader:

- 1. **Sekretessmarkering**, som innebär att personens uppgifter markeras som känsliga.
- 2. **Kvarskrivning**, man fortsätter att vara skriven på en adress där man inte längre bor.
- 3. **Fingerade personuppgifter** (”ny identitet”).

- Enligt 5:4 § p. 3 HSLF-FS ska det finnas rutiner som säkerställer att journal går att föra för patienter med skyddad identitet.

- Regeln har ofta felaktigt uppfattats som ett undantag från, eller begränsning av journalföringsplikten för dessa patienter. Det är alltså inte korrekt. Vad som tvärtom sägs är att alla ordinarie regler ska gälla. Hur detta ska säkerställas överlämnas till vårdgivarna att avgöra.

- Det finns dock inte längre något uttryckligt krav på att patientens namn ska antecknas i journalen. Man talar istället om ”entydig identifikation” (5:3 § p. 1 HSLF-FS 2016:40).

Martha Gurmu

www.fysioterapeuterna.se