Policy för Personuppgiftsskydd

1 Inledning

Mediqs policy för personskydd beskriver på ett övergripande sätt de regelverk som gäller inom Mediq vid hantering av personuppgifter.

Om du har frågor rörande denna policy, allmänt om dataskydd eller misstänker oegentligheter kring vårt dataskydd ska frågan ställas till vårt Dataskyddsombud på personuppgifter@mediq.com.

2 Mission

Mediqs mission är att vara en pålitlig leverantör till hälso- och sjukvården och bidra till att människor får ett så bra liv som möjligt. Mediq är en pålitlig partner inom sjuk- och hälsosektorn och försäkrar i nära samarbete med våra leverantörer att patienten är fokus i detta arbete. Detta förutsätter också att Mediq respekterar anställdas, partners och patienters rätt till dataskydd.

Skyddet rörande behandling av personuppgifter är en grundläggande rättighet. Denna Policy för personuppgiftsskydd baseras på den Europeiska dataskyddslagen ”EU General Data Protection Regulation (2016/679)”.

3 Ansvar

Alla medarbetare på Mediq är ansvariga för att man som anställd följer gällande lagar och förordningar.

Genom denna policy för personuppgiftsskydd säkerställs att alla anställda är införstådda med gällande regelverk.

Mediq Sveriges ledning är ytterst ansvarig för att säkerställa att gällande lagstiftning och förordningar följs tillsammans med denna policy för personuppgiftsskydd.

Dataskyddsombudet är ansvarig för att etablera rutiner och aktiviteter för att säkerställa att denna policy efterlevs.

4 Principer

Mediq förbinder sig att och ansvarar för att följa nyckelprinciperna kring dataskydd, vilket innebär att vid behandling av personuppgifter ska följande gälla:

1. Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.
2. De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.
3. De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.
4. De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas, raderas eller rättas utan dröjsmål.

5. De får inte förvaras under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.
6. De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

När Mediq utvecklar och väljer applikationer/tjänster till verksamheten som ska användas för att behandla personuppgifter ska hänsyn tas till ovanstående principer i ett så tidigt skede som möjligt. Hänsyn kan tas till genomförandekostnad och behandlingens art samt risker.

Lämpliga tekniska och organisatoriska åtgärder ska genomföras för att säkerställa att endast personuppgifter som är nödvändiga behandlas. Skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter inte blir tillgängliga för fler personer än nödvändig för hanteringen.

4.1 Konsekvensbedömning

En konsekvensbedömning ska genomföras innan Mediq påbörjar en systematisk och omfattande behandling av personuppgifter som kan få rättsliga följder eller på annat sätt har betydande påverkan för de registrerande. Dataskyddsombudet ska bistå i denna typ av bedömning.

5 Laglig grund för behandling

Behandling av personuppgifter är endast laglig om minst ett av följande villkor är uppfyllt:

1. Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas.
2. Behandlingen är nödvändig för att fullgöra ett avtal eller inför ett avtal.
3. Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som Mediq har.
4. Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan person.
5. Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
6. Behandlingen är nödvändig för ändamål som rör Mediqs eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Behandling av personuppgifter av särskilt känslig karaktär är förbjuden om inte följande gäller:

1. Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter.
2. Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.
3. Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård och behandling.

Om behandlingen grundar sig på samtycke, ska Mediq kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter.

6 Register

Mediq ska föra ett skriftligt register över aktiviteter där personuppgiftsbehandlingar utförs inom företaget.

Detta register ska innehålla följande uppgifter:

1. Namn och kontaktuppgifter för Personuppgiftssansvariga samt dataskyddsombudet på Mediq samt i de fall aktiviteten utförs av en extern part, dennes kontaktuppgifter.
2. Syftet med behandlingen.
3. En beskrivning av de kategorier/grupper som registreras.
4. En beskrivning av de personuppgifter som registreras.
5. De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut
6. Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
7. Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder

7 Skyldigheter vid anlitande av personuppgiftsbiträde

När Mediq i egenskap av personuppgiftsansvarig anlitar ett personuppgiftsbiträde ska Mediq tillse att tillräckliga garantier ges om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen lever upp till lagkrav och denna policy.

Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av Mediq. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

När uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal som anger föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter.

Om Mediq anlitar ett personuppgiftsbiträde är Mediq ansvarigt för att de följer denna policy på samma sätt som Mediq.

8 Den registrerades rättigheter

8.1 Rätt till registerutdrag

Du som registrerad kan begära ett registerutdrag där du anger vilken information du vill ta del av. Mediq ska besvara dina önskemål utan onödigt dröjsmål inom rimlig tid, normalt inom en (1) månad. Om Mediq av någon anledning inte kan uppfylla dina önskemål, ska detta motiveras på ett sakligt sätt. Registerutdrag begärs skriftligen och kommer att skickas till din folkbokföringsadress.

8.2 Rätt till begäran om rättelse av dina personuppgifter

Mediq ansvarar för att personuppgifterna vi behandlar är korrekta, men du som registrerad har också rätt att komplettera med uppgifter som saknas och som är relevanta. Om du upptäcker felaktig information om dig har du rätt att begära att få detta korrigerat.

8.3 Rätt till begäran om radering av dina personuppgifter

Dina personuppgifter sparas så länge det är nödvändigt enligt lag, exempelvis Bokföringslagen.

Som registrerad har du rätt att begära att utan onödigt dröjsmål få information raderad. Mediq kommer då att bedöma om det är möjligt utifrån gällande lagstiftning.

9 Hantering av en personuppgiftsincident

Mediq har skyldighet att informera Datainspektionen inom 72 timmar efter att en incident har upptäckts. Mediq kommer även att göra vad som är möjligt för att minimera den eventuella skada som kan ha uppstått för den registrerade samt informera den registrerade om vad som har inträffat.

10 Överföring av personuppgifter till utlandet

För överföring av personuppgifter till länder utanför EU och EES (så kallad tredjelandsöverföring) gäller särskilda regler. Dataskyddsförordningen innebär att alla EU:s medlemsstater har ett likvärdigt skydd för personuppgifter och personlig integritet. Detta gäller även EES-länderna Norge, Island och Liechtenstein. Därför kan personuppgifter föras över fritt inom detta område utan begränsningar. Eftersom det inte finns några generella regler som ger motsvarande garantier utanför EU och EES har man ansett att överföring (inkl. utnyttjande av molntjänster) till sådana länder bara får ske under särskilda förutsättningar.

Mediq tillåter enbart överföring av personuppgifter till länder utanför EES samt europeiska dotterbolag till USA-baserade företag efter godkännande från Mediqs dataskyddsombud på koncernnivå.

Vid överföring utanför EU och EES gäller följande tillämpliga regelverk:

1. Följande länder har EU-kommissionen beslutat säkerställer en fullgod skyddsnivå: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
2. Regelverk rörande överföring till USA-baserade företag: http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm.
   Att överföra personuppgifter till ett USA-baserat företag eller europeiska dotterbolag till USA-baserade företag är bara tillåtet om företaget har en ”active Privacy Shield certifiering” och certifieringen täcker de berörda uppgifterna.
3. Överföringar där ett undantag som anges i gällande lagar och förordningar gäller (till exempel uttryckligt samtycke från den registrerade).

11 Dataskyddsombud på koncernnivå

Mediq har utsett ett Dataskyddsombud på koncernnivå som ska ha expertkunskap om lagar och praxis för dataskydd och möjligheten att uppfylla de uppgifter som beskrivs i denna Policy för personuppgiftsskydd. Koncernens dataskyddsansvarig samverkar med det lokala dataskyddsombudet och har främst följande uppgifter:

1. Att informera och ge råd till det lokala dataskyddsombudet rörande dataskyddsfrågor.
2. Att övervaka överensstämmelse med gällande lagar och förordningar och denna policy för personuppgiftsskydd tillsammans med det lokala dataskyddsombudet.

3. Att ge råd vid frågor kring konsekvensbedömningen av personuppgiftsskyddet och övervaka dess resultat.
4. Att samarbeta med tillsynsmyndigheterna den lokala dataskyddsombudet.
5. Upprättande och kontroll av efterlevnad av Policy för personuppgiftsskydd på koncernnivå och relaterad dokumentation.
6. Att hålla Mediqs koncernledning uppdaterad om personuppgiftsskydd, överensstämmelse, risker och problem.