

Fotokopians överensstämmelse
med originalet intygas: *Usp*

Örebro läns landsting
Box 1613
701 16 Örebro

Förhandskontroll enligt 41 § personuppgiftslagen (1998:204)

Anmälan

Örebro läns landsting har den 25 oktober 2007 inkommit med en anmälan om behandling av personuppgifter om genetiska anlag, som har framkommit efter genetisk undersökning, för förhandskontroll.

Av anmälan framgår följande.

Personuppgifterna skall behandlas inom ramen för en forskningsstudie om behandling för att förebygga återinsjuknande i depression.

De registrerade kommer att informeras om behandlingen av personuppgifter och samtycke till behandlingen kommer därefter att inhämtas från samtliga registrerade.

De genetiska undersökningarna kommer att genomföras först efter granskning av etikprövningsnämnd.

Skäl för beslutet

Personuppgiftslagen innehåller inget krav på skriftligt samtycke. De registrerades samtycke måste dock vara uttryckligt. Av de registrerades samtycke måste det framgå att samtycket omfattar den datoriserade behandling av personuppgifter som skall utföras i projektet. Det är inte tillräckligt att de registrerade samtycker enbart till att delta i projektet som sådant. Det är den personuppgiftsansvarige som vid en eventuell tvist har bevisbördan för att ett giltigt samtycke har inhämtats.

Därför krävs – för att behandlingen av personuppgifter inom ramen för forskningsstudien ska vara förenlig med personuppgiftslagens bestämmelser – att samtyckesformuläret ändras. Vidare kan ett tillägg i patientinformationen vara nödvändig.

Det rör sig om följande ändring och tillägg:

- Örebro läns landsting måste på samtyckesformuläret inhämta de registrerades uttryckliga samtycke till att deras personuppgifter, däribland uppgifter om genetiska anlag, behandlas inom ramen för forskningsstudien.

- Örebro läns landsting har i anmälan för förhandskontroll uppgett att personuppgifterna kan komma att lämnas ut till samarbetande forskare. Om detta innebär att personuppgifterna kan lämnas ut till forskare utanför Örebro läns landsting, måste i patientinformationen anges att personuppgifterna kan komma att lämnas ut till forskare utanför Örebro läns landsting.

Förutsatt att samtyckesformuläret (och eventuellt patientinformationen) ändras på detta sätt, är personuppgiftsbehandlingen inom ramen för studien förenlig med personuppgiftslagen.

Vidare rekommenderar Datainspektionen att uttrycket "personuppgiftsansvarig" används i patientinformationen istället för uttrycket "PUL-ansvarig".

Med hänsyn till att de personuppgifter som skall behandlas inom ramen för forskningsstudien är mycket integritetskänsliga anser Datainspektionen att det finns anledning att meddela beslut om särskilda säkerhetsföreskrifter för behandlingen.

Beslut

Datainspektionen meddelar följande föreskrifter om den säkerhetsnivå som skall tillämpas vid behandlingen av personuppgifter inom ramen för forskningsstudien.

Följande skall iakttas beträffande IT-säkerheten.

Säkerhetspolicy

Den personuppgiftsansvarige skall se till att det finns en fastställd säkerhetspolicy som även omfattar forskningsprojektet.

Utbildning och information

Alla som får tillgång till personuppgifter om genetiska anlag skall få information och relevant utbildning om gällande säkerhetsrutiner.

Autentisering/Behörighetskontroll

Det skall finnas tekniska system för autentisering och behörighetskontroll för att styra åtkomsten till personuppgifterna. Behörigheten skall begränsas till dem som behöver uppgifterna för sitt arbete. Användaridentitet och lösenord skall vara personliga och får inte överlåtas på någon annan. Det skall finnas rutiner för tilldelning av behörigheter. Om personuppgifterna är åtkomliga via ett öppet nätverk, såsom Internet, krävs stark autentisering, till exempel engångslösenord, användarcertifikat (e-legitimation) eller motsvarande.

Datakommunikation

Om personuppgifter överförs via öppet nät skall uppgifterna skyddas med kryptering. Utrustning som ansluts till Internet eller annat öppet nät skall skyddas så att obehörig trafik förhindras, till exempel med hjälp av brandvägg.

Om personuppgifter lagras på en dator som är åtkomlig från ett öppet nät skall uppgifterna lagras krypterat.

Behandlingshistorik/Loggar

Om fler än en person har åtkomst till personuppgifterna skall det finnas loggar eller annan behandlingshistorik som underlag för att kunna följa upp åtkomsten i efterhand. Av detta underlag skall det gå att utläsa vem som har haft åtkomst, tidpunkten för åtkomsten samt vilka uppgifter användaren haft åtkomst till.

I syfte att upptäcka eventuell obehörig åtkomst till uppgifterna skall det finnas rutiner för systematisk uppföljning av behandlingshistoriken i följande fall.

Om uppgifterna är åtkomliga för många användare och det

1. rör sig om ett stort antal uppgifter om varje person *eller*
2. om uppgifterna rör ett stort antal personer.

Åtkomstskydd/Tillträdeskontroll

I bärbara datorer och på löstagbara lagringsmedier skall personuppgifterna vara krypterade på ett sådant sätt att obehöriga inte kan ta del av uppgifterna.

I syfte att skydda uppgifterna från obehörig användning, påverkan eller stöld skall annan datorutrustning – i vilken personuppgifter lagras eller genom vilken man kan få åtkomst till uppgifterna – vara inlåst när den inte står under den personuppgiftsansvariges uppsikt. Alternativt skall uppgifterna vara krypterade.

Skydd mot skadliga program

Åtgärder skall vidtas för att minska risken för att personuppgifterna förstörs eller sprids till obehöriga med hjälp av skadlig programvara.

Säkerhetskopiering

Personuppgifterna skall regelbundet överföras till säkerhetskopior. Kopiorna skall förvaras avskilt, vara väl skyddade och rutinmässigt testas för att säkerställa så att personuppgifterna kan återskapas efter en störning. Skyddet för kopiorna skall ha samma säkerhetsnivå som skyddet för originalen.

Utplåning

När fasta eller löstagbara lagringsmedier som innehåller personuppgifter inte längre skall användas för sitt ändamål skall lagringsmedierna förstöras. Alternativt skall personuppgifterna raderas med hjälp av särskild programvara på sådant sätt att de inte kan återskapas.

Reparation och service

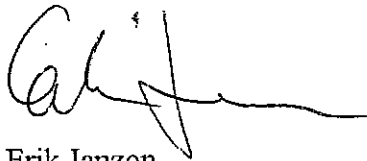
När reparation och service av datorutrustning utförs av annan än den personuppgiftsansvarige skall avtal om säkerheten träffas med serviceföretaget så att skyddet för personuppgifterna inte försvagas.

Vid servicebesök skall lagringsmedier som innehåller personuppgifter avlägsnas. Är det inte möjligt skall servicen ske under den personuppgiftsansvariges överinseende.

Service via datakommunikation får endast ske krypterat och efter säker identifiering av den som utför servicen. Servicepersonal skall ges åtkomst till systemet endast vid servicetillfället och endast till de delar som behövs för servicen. Kommunikationsingångar och särskilda administrationskonton för service skall vara stängda när service inte pågår.

Hur man överklagar

Om Ni vill överklaga beslutet ska Ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som Ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades för att kunna prövas. Datainspektionen sänder överklagandet vidare till Länsrätten i Stockholms län för prövning om inspektionen inte själv ändrar beslutet på det sätt Ni har begärt.



Erik Janzon

Kopia till:

Axel Nordenskjöld
Allmänpsykiatriska kliniken
Universitetssjukhuset
701 85 Örebro

Personuppgiftsombudet Bo Andersson
Örebro läns landsting
Box 1613
701 16 Örebro