7KULL. 5

Datainspektionen

Datum
2007-02-09

Dnr
52-2007

Region Skåne
Universitetssjukhuset MAS
205 02 MALMÖ

Förhandskontroll enligt 41 § personuppgiftslagen (1998:204)

Anmälan

Region Skåne har genom Institutionen för Diabetes och endokrinologi, CRC, UMAS, den 15 januari 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 den s.k. ANDIS-studien – "Alla Nya Diabetiker i Skåne". Studiens målsättning är att klassificera diabetessjukdom i undergrupper för att åstadkomma en bättre individualiserad vård. DNA-prov tas för analys av genetiska faktorer som kan hjälpa till att klassificera diabetestypen.

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

Studien har godkänts av forskningsetisk kommitté vid Lunds universitet.

Skäl för beslutet

Eftersom behandlingen av de känsliga personuppgifterna om genetiska anlag som skall utföras inom ramen för studien endast kommer att ske sedan samtliga registrerade har fått den information om behandlingen som krävs enligt personuppgiftslagen och därefter lämnat sitt uttryckliga samtycke är behandlingen förenlig med personuppgiftslagens bestämmelser.

Datainspektionen vill dock påpeka att om känsliga personuppgifter om släktingar till patienterna kommer att hanteras automatiserat i studien skall även släktingarna lämna sitt samtycke till hanteringen enligt personuppgiftslagen.

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

Postadress: Box 8114, 104 20 STOCKHOLM
Besöksadress: Fleminggatan 14, plan 9
Webbplats: http://www.datainspektionen.se

E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

Beslut

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

Följande skall iakttas beträffande IT-säkerheten.

- Åtkomstskydd:
När datorutrustning och löstagbara datamedier inte står under uppsikt skall utrustningen och medierna låsas in för att skyddas mot obehörig användning, påverkan och stöld. I annat fall skall personuppgifterna krypteras.

I bärbara datorer skall personuppgifterna på fasta och löstagbara lagrings-medier alltid vara krypterade.

-Säkerhetskopia:
Personuppgifterna skall regelbundet överföras till säkerhetskopior. Kopiorna skall förvaras avskilt och väl skyddade så att personuppgifterna kan återskapas efter en störning.

- Behörighetskontroll:
Ett tekniskt system för behörighetskontroll skall styra åtkomsten till person-uppgifterna om datorn används av mer än en person. 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.

- Loggning:
Åtkomst till personuppgifter skall kunna följas upp i efterhand genom en maskinell logg eller liknande maskinellt underlag om datorn används av mer än en person. Av detta underlag skall framgå vem som har haft åtkomst, tidpunkten för åtkomsten samt till vilken persons uppgifter åtkomsten har skett. Underlaget skall kontrolleras i tillräcklig utsträckning.

- Datakommunikation:
Anslutning för extern datakommunikation skall skyddas med motringning eller annan teknisk funktion som säkerställer att uppkopplingen är behörig.

Personuppgifter som överförs via datakommunikation utanför lokaler som kontrolleras av den personuppgiftsansvarige skall skyddas med kryptering.

- Utplåning:
När fasta eller löstagbara lagringsmedier som innehåller personuppgifter inte längre skall användas för sitt ändamål skall lagringsmedierna förstöras. Alter-nativt skall personuppgifterna raderas på sådant sätt att de inte kan återskapas.

- Reparation och service:
När reparation och service av datorutrustning utförs av annan än den person-

uppgiftsansvarige skall avtal om säkerheten träffas med serviceföretaget.

Vid servicebesöket skall lagringsmedier som innehåller personuppgifter avlägsnas. Är detta inte möjligt skall servicen ske under den personuppgifts-ansvariges överinseende.

Service via datakommunikation får endast ske efter säker identifiering av den som utför servicen. Servicepersonal skall ges åtkomst till systemet endast vid servicetillfället. Finns separat kommunikationsingång för service skall den vara stängd när service inte pågår.

Hur man överklagar

Om Ni vill överklaga beslutet skall Ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som Ni begär. Överklagandet skall 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.

På Datainspektionens vägnar

Katja Isberg Amnäs

Kopia till:
Personuppgiftsombudet
Britt Lagerlund
Universitetssjukhuset MAS
205 02 MALMÖ

PUO-förvaltaren
Universitetssjukhuset MAS
Lena Larsson
205 02 MALMÖ

Regionala etikprövningsnämnden i Lund
Box 133
221 00 LUND

Professor Leif Groop
Inst. för diabetes och
endokrinologi
CRC, UMAS
205 02 MALMÖ