

The Icelandic Health Sector Database

Professor Páll Hreinsson
Chairman of the board of the Data Protection Authority in Iceland

1. Introduction.

It was in the 1970s that the first concrete suggestions were voiced about establishing a database containing information on health and genetic materials so as to be able to do research on diseases and disorders with a genetic component. At that time, most people regarded this idea as completely unrealistic. Only a few decades later, however, legislation was enacted in Iceland to open the way for just such a database, and it is expected to go into operation next year.

In the short time I have available here, I would like to give an account of some of the issues that caused the most controversy when the legislation on the Health Sector Database was being debated in Iceland. Then I will describe briefly how the database is expected to function. But first, I would like to examine a few points that have given rise to a great deal of misunderstanding.

2. The three databases.

The Icelandic Health Sector Database Act has been the subject of extended discussions all over the world, as it has been possible to learn a lot from the questions that arose when it was under debate. However, it should be borne in mind that what has been said about the Health Sector Database has not always been based on the facts. This is perhaps not surprising, since the Health Sector Database Act is very unclear and its meaning is difficult to grasp without reading all the explanatory materials. One of the main sources of misunderstanding is the fact that the statistical data which the licensee intends to sell will be derived not only from the Health Sector Database but from two other databases as well.

First there is the Health Sector Database, which contains health data from medical records. Then there is a database that contains genetic information, and thirdly there is a database with genealogical information. Each of these three databases is subject to different legal provisions. The Health Sector Database itself is subject to the world-famous and controversial Health Sector Database Act, No. 139/1998.¹ The genetic database is covered by the Act on Biobanks and the Patients' Rights Act, the Data Protection Act and other legislation, and the genealogy database is covered by the Data Protection Act. The Health Sector Database Act contains provisions allowing for the interconnection of all these databases in order to generate statistical responses to queries. I will come back to this point later on.

3. Written consent.

The proposal to enact legislation on a Health Sector Database in Iceland sparked off a heated and bitter argument that has in fact gone on for the past 4 years. One of the main issues was whether the data was to be derived from medical records in accordance with written consent of each individual patient, or whether a law should be passed allowing for the transfer of such data to the database without the patient's consent.²

Many of the opponents of the database demanded that medical data should be gathered on the basis of the informed consent of the patient, and not only this, but that the declaration of consent

¹ The Act Health Sector Database Act, No. 139/1998 in English is in the public domain and is published on the DPA's website <http://www.personuvernd.is/tolvunefnd.nsf/pages/english>

² See Vilhjálmur Arnason: "Coding and Consent": Moral Challenges of the Database Project in Iceland" which has been accepted for publication in Bioethics.

should meet the conditions of the Helsinki Declaration. For the past ten years, genetic research in Iceland has been subject to such consent when it involves taking biosamples from living persons.

The term "informed consent" in the sense of the Helsinki Declaration, has, in Iceland at any rate, been interpreted as meaning that before the individual gives his formal consent, he must be informed thoroughly about many details of the specific study in which he is about to take part. The key point here is therefore that the information given concerns one specific scientific study. But it was clear that as the act was structured, it would never be possible to inform the patient about every individual study that was intended to carry out using the data that would be put in the database. It would only be possible to inform patients of the purpose of the processing. For this reason, many people came to the conclusion that in the case of a database of this type, the giving of consent could not, in the nature of things, meet the demands associated with the Helsinki Declaration as it had been applied in Iceland.

On the other hand, it was also pointed out that even though the intention was to obtain patients' written consent after they had been informed of the purpose of the processing, the definition of the purpose given in the Act was so broad that patients would find it difficult to understand what, in fact, they were giving their consent to.

The purpose of the processing is defined as follows in Article 10 of the Act:

"Data recorded or acquired by processing on the health-sector database may be used to develop new or improved methods of achieving better health, prediction, diagnosis and treatment of disease, to seek the most economic ways of operating health services, and for making reports in the health sector."

In the debate on the Act when it was presented as a bill, the Data Protection Authority stressed that the only way individual privacy and the right of self-determination could be protected would be to have a provision in the Health Sector Database Act requiring patients' written consent for the gathering of data. On the other hand, this would mean that the purpose of the processing would have to be defined as clearly as possible and clear provision would have to be made for patients to withdraw their consent. The Data Protection Authority also emphasised how new and unfamiliar this research technique would be, and also how little was known about the implications of this type of research, both for Iceland as a small and homogeneous nation and also for those individuals to whom the data referred.

The Data Protection Authority argued that in terms of the sensitive nature of the data to be included in the database, and how serious the implications of it might be, it was not right for the legislature to act paternalistically and decide unilaterally that medical data should be entered into the database automatically.

There is not time here to survey all the arguments that were advanced as to why processing of medical data in a database of this type should be based on specific, written consent of the patients. But to make a long story short, parliament decided that the transfer of data should be subject not to specific, written consent, but to presumed consent. The main reason given for deciding on this arrangement was that it would be virtually impossible to obtain written consent from all patients. In order to meet the criticisms of opponents of the database, the Icelandic Parliament decided to establish a procedure by which people could choose not to participate in the project by submitting a written request not to have their medical data included in the database. According to the latest information, more than 20,000 people, out of the total population of 280,000, have exercised this right. The Director-General of Public Health maintains a register of those who ask not to have their data included in the database. The other point that the Icelandic Parliament decided on was to demand a very high level of security in the operation of the database. For example, all data to be included in the database must be encrypted with strong encryption.

4. Problems connected with the procedure for non-participation.

After the Act was passed, doubts were expressed as to whether it was compatible with Article 71 of the Icelandic Constitution and Article 8 of the European Convention on Human Rights. An example of the criticisms made regarding the procedure for non-participation is that elderly and seriously ill patients are often not able to decide whether or not they want to participate in the database. Children and other individuals who are not legally competent to manage their own affairs are dependent on

their guardians as to whether their right of non-participation is exercised. Disputes have also arisen as to whether an individual is able to refuse to have data on a deceased child or parent entered into the database. A case on this question is currently being heard in Iceland.

The main criticism, however, concerned the situation of somebody whose data had already been entered in the database, but then decided they wanted to withdraw from it. The question was raised whether the arrangement on this point was compatible with the Constitution and the European Convention on Human Rights. The rule was that data already entered would not be deleted afterwards, even though the individual concerned withdrew from further participation. Such a withdrawal would only mean that no further data on the individual would be entered, but data already in the database would not be affected. The Icelandic Parliament had decided on this arrangement because it considered that the scientific value of the database would be undermined if it were to be affected retroactively by withdrawals.

Many people were of the opinion that the licensee should have been made to accept this risk, since in fact it was not likely that the scientific value of the database would be seriously affected unless large numbers of people withdrew their data from it. A withdrawal procedure that does not permit the deletion of data that has already been entered is of very little value.

5. The Health Sector Database Act and Directive No. 95/46/EC.

Another point of dispute when the Act was passed was whether Directive No. 95/46/EC should be taken into account. There was disagreement as to whether the data to be entered in the database should be regarded as personal data in the sense of section *a* of Article 2 of the Directive. The lawyers who drafted the bill on the Health Sector Database did not regard these data as personal data, firstly because the personal identification features were to be encoded unidirectionally, and secondly because the only data that would be released from the database would be in statistical form, with no identification of individual persons being possible. The conclusion was therefore that the majority of the Icelandic Parliament considered that Directive No. 95/46/EC did not prevent the passing of the Act. Nor did the EFTA Surveillance Authority consider there was any reason to raise an objection to the Act on these grounds. It is not impossible that this might be put to the test later, but it should be borne in mind that if the data in the database are regarded as personal data in the sense of section *a* of Article 2 of the Directive, there would then arise the question of whether the database would come under the exemption provisions of paragraphs 3 and 4 of Article 8 of the Directive. Opinion has been divided on this point too.

6. Announcement of a case to be brought before the courts.

A non-governmental organisation, the Association of Icelanders for Ethics in Science and Medicine (Mannvernd), has announced its intention of bringing an action before the Icelandic courts to test whether the failure to demand written consent for the inclusion of data in the database is compatible with the Constitution and the European Convention on Human Rights. If such an action is brought before the courts in Iceland, not to mention the possibility that it might go as far as the European Court of Human Rights, this could throw light on the minimum human rights guaranteed to the individual under Article 8 of the Convention in connection with such databases. The situation in law is far from clear.

7. A change in position by the licensee.

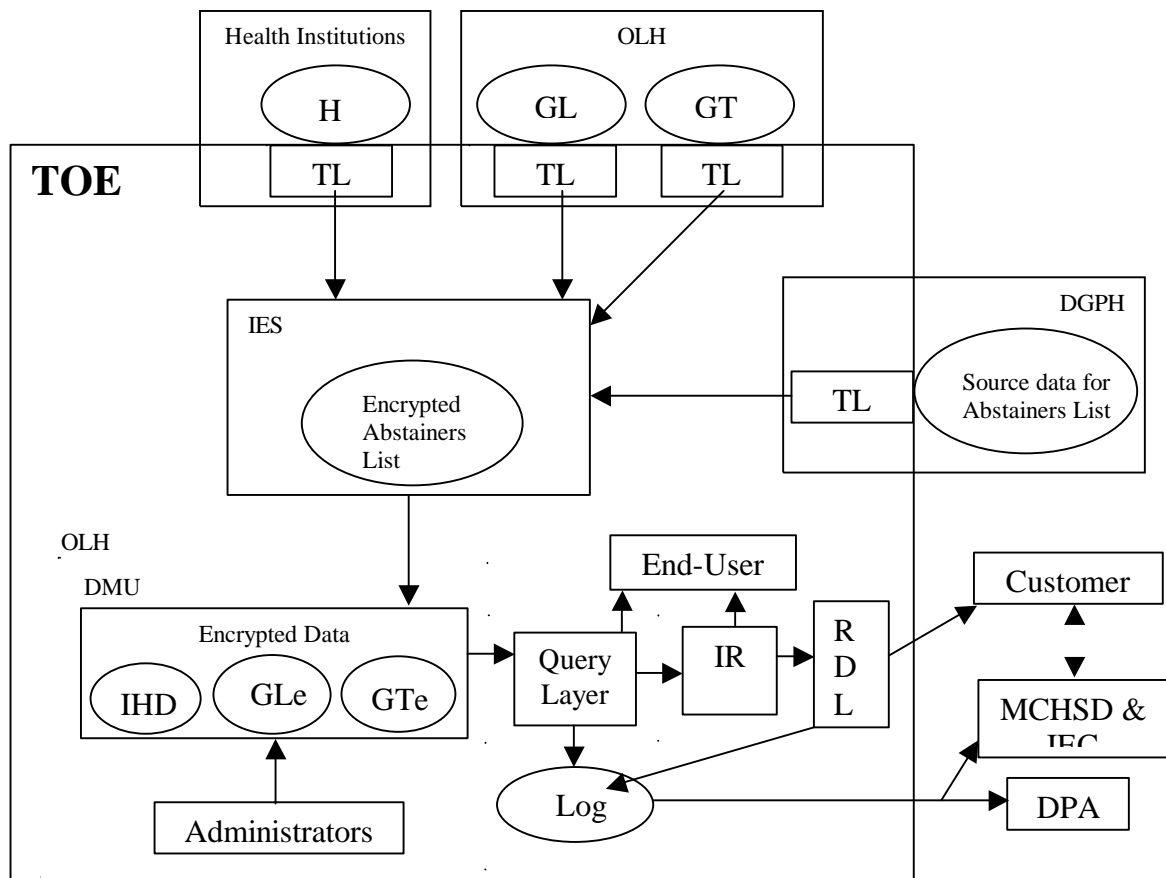
On 27 August this year, the licensee announced a change in position on certain aspects of the database. The licensee and the Icelandic Medical Association then made an agreement to the effect that in cases where a person decides to withdraw from participation in the database, the data on that person will then be deleted. Also, the licensee declared that when the World Medical Association's declaration on the scientific ethics of databases is made public, it will be taken into account when changes are made to the database. If the licensee stands by this undertaking, then this clearly marks a watershed in the history of the database. But at the moment it is difficult to say anything about the contents of the WMA's declaration and consequently the effect that it will have on the Health Sector Database.

8. How is medical data put into the database?

To form a better understanding of how the Health Sector Database is intended to function, it is useful to look at a simplified diagram. Medical data is sent to the database by health institutions and private medical practitioners. Under the Act, the licensee supplies these institutions and practitioners with special software for a harmonised data system to process and store medical records. Under the Act, this system is regarded as part payment for the data. The licensee is required to pay all expenses in connection with entering older data into the system and processing the information so that it can be transferred to the database.

Under the Act, those who handle data must be employees of the relevant medical institutions or private medical practitioners and must be qualified to work in the health services. One of the reasons for setting this condition was to prevent the licensee’s employees from gaining access to the data before it is transferred to the database.

The licensee must make a contract with health institutions or private practitioners before it can obtain data from them. Article 7 of the Act states that health institutions are to confer with the physicians' council and specialist management of the relevant institution before contracts are concluded with the licensee. The licensee has already made contracts with the largest hospitals in Iceland on the transfer of medical data to the Health Sector Database.



The Icelandic Health Sector Database

Article 7 of the Act states that medical data is to be transferred in an encrypted form in order to guarantee security. Before being released from the health institution, the personal identification features are encrypted unidirectionally, while the medical data themselves are encrypted with a key. The data is then sent to the encryption unit of the Data Protection Authority. The first thing to be done there is that data on individuals who have chosen not to participate in the project are removed. A register of these individuals is kept by the Director-General of Public Health. This is done at this point in the process so as to prevent it being known, for example by employees in the health service institutions, who has chosen not to participate in the database. Only three employees of the office of the Director-General of Public Health have access to this register. After the data on these individuals has been removed, the personal identification features are encrypted again and the data is forwarded to the database. No data is stored in the Data Protection Authority's encryption unit, and the only way data can enter the database is via the encryption unit. The Data Protection Authority was entrusted with the operation of the encryption unit under the Act. The authority criticised this arrangement, as it did not consider it appropriate that it should carry out this processing function, on the one hand, while monitoring it on the other.

9. How is processing carried out in the database?

It is envisaged that genetic data will be obtained with written consent. Both genetic and genealogical data will then be encrypted and transferred to the database in the same way as medical data.

Under Article 10 of the Health Sector Database Act, the licensee is permitted to carry out processing in the database of the medical data recorded there providing that steps are taken to ensure that when this is done, and when the data are connected with other data, it is not possible to trace them to identifiable individuals. The notes to the act when it was presented as a bill state that the database is a statistical database and that the results of processing are only to be presented in a statistical form in which individuals can not be identified. Article 10 of the Act also states that the licensee is to develop methods and protocols that will meet the requirement set by the Data Protection Authority regarding anonymity when data in the Health Sector Database is connected to data from the genetic and genealogical databases.

10. Security of the database.

Article 5 of the Act states it as a condition for the operation of the Health Sector Database that the technical, security and organisational standards meet the requirements set by the Data Protection Authority. Article 12 of the Act commissions the Data Protection Authority with monitoring the creation and operation of the database regarding the recording and handling of personal data, and the security of the data, and with monitoring to ensure compliance with the conditions it sets.

The DPA sought extensive consultation, from domestic and foreign specialists in the field of database security, on how best to fulfill this obligation. On the basis of their advice, the DPA decided to base its evaluation of the database on an international standard, ISO/IEC 15408, which is often referred to as the 'Common Criteria'. The standard calls for issuing specifications of the security requirements for the project, which are based on the Act. These specifications are referred to as the 'Security Target' and were issued by the DPA as version 1.0 in January 2000. The current version is 1.4 and was issued in January 2001. The 'Security Target' is the document against which the database is audited. It is in the public domain and is published on the DPA's website.³

The 'Security Target' and 'Common Criteria' call for a variety of security requirements to be incorporated into the system. They cover everything from the physical security, such as the building that will house the system and the machinery used, to the vetting of employees, the cryptographic systems employed, password usage, etc. Furthermore, an array of requirements are designed to provide assurance that the system is in fact secure. These include running rigorous tests on the system through rigorous tests and probing it for security vulnerabilities. The security requirements are designed to meet threats from skilled attackers launching powerful attacks, both from within the system and from the outside. The audit is conducted by the DPA with the assistance of Icelandic technical experts and a British security consultancy firm, CMG UK Ltd. It began this summer and is

³ <http://www.personuvernd.is/tolvunefnd.nsf/pages/english>

currently scheduled to end early next year. The audit methodology, however, calls for the licensee to decide how rapidly it presents for evaluation the required evidence of compliance. It therefore depends on the licensee when this evaluation will end.

It should be pointed out that the Data Protection Authority is not the only official body involved in monitoring the Health Sector Database. A special committee was established under Article 6 of the Act, its role being to ensure that the creation and operation of the database are in keeping with the terms of the Act, the regulations issued under the Act and conditions laid down in the operation licence in so far as this does not fall within the ambit of the Data Protection Authority. Another committee, the interdisciplinary ethics committee, is to assess studies carried out within the licensee's company and handle queries received. The committee's evaluation must reveal that there is no scientific or ethical reason to prevent the study in question being carried out or the queries being processed from the database.

11. Conclusion

If we turn to the international conventions and European directives on genetic data, we have to admit that we are not yet really equipped with the rules that are needed on research using large-scale DNA collections.

My view is that it is very important to harmonise regulations in this area in the EEA. Carefully grounded regulations on the conditions governing genetic research in the health sector using large databases are not only of significance regarding the personal privacy and fundamental rights of sample donors. Such regulations can also be seen as defining the operational framework of companies that are in competition in this field.

Huge investments will be made in genetic research in the years ahead, and unless there are uniform regulations on research using large-scale DNA collections, then the companies active in this field will not be operating in the same competitive environment. One possible consequence of this situation would be that research companies would simply flock to the countries whose parliaments set the lowest standards regarding privacy.

I believe that future developments will depend very much on whether we manage to harmonise our rules in this area. But let us bear in mind that the longer we take arriving at a conclusion on the basic rules that should apply in this area, the more difficult it will be to implement such rules.

If I try to sum up what is unique about the Icelandic Health Sector Database, it is first and foremost that medical data on an entire nation are assembled in a single database that is operated by a sole licensee for the purpose of scientific research, and that data is entered in the database without the consent of the patients. Iceland's parliament considered that explicit consent was not necessary since the security of the data would be ensured by the use of the latest technology and the strictest safety requirements.

If we stop and consider this point, the question arises: Is this the shape of things to come? Will technical solutions replace the right of self-determination and other associated human rights and make it unnecessary to obtain consent of those concerned for the processing of perhaps even the most sensitive personal data? Is this what we are moving towards? I hope not.