



UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

Brief Report on the Data Protection Audit

**Data Processing Infrastructure Concept
of the Schering Corporation
for the Secure Pseudonym Storage and Keeping of
Blood and Tissue Samples intended for genetic analyses**

Developed by

**The AG Kommunikationssysteme at the Institut für Informatik und
Praktische Mathematik
Professor Norbert Luttenberger,
Christian-Albrechts-Universität zu Kiel**

**English version of the audit report, approved by the Independent
Centre for Privacy Protection**

I. Object of the Data Protection Audit

The object of the data protection audit is a security concept that was created by the AG Communications Systems at the Institute for Computer Science and Practical Mathematics; Professor Norbert Luttenberger, at the Christian Albrechts University in Kiel (CAU) on behalf of and in cooperation with the Schering AG company. This security concept refers to a project by Schering AG for **conducting pharmacogenetic studies**. In the context of pharmacogenetics, blood and tissue samples of subjects are tested to determine the relationship between certain genetic information and the effect of pharmaceutical products upon it.

Schering AG conducts pharmacogenetic studies which are supported by an IT infrastructure. These pharmacogenetic studies are conducted **in addition to clinical studies**. When conducting these studies, the subject's genetic data from blood or tissue is collected and subsequently compared with the medical data from the participants which has been obtained in the context of clinical studies.

This process, known as the **GENOMatch-Project**, has the task to establish and operate the necessary IT infrastructure for pharmacogenetic studies. In particular, the GENOMatch-Project should incorporate the data protection measures which are required in this setting. The project is divided into three sections. The sections of GENOMatch are designed as follows:

Section 1: The establishment of a pharmacogenetic database, meaning the collection and management of blood and tissue samples – the sample and save strategy.

Section 2: The generation and secure storage of pseudonymous genetic and clinical data.

Section 3: Support for the statistical analysis of the data, meaning „data matching“ of clinical and genetic data (creation of aggregated data) in the context of pharmacogenetic studies.

The existing data protection audit refers to the first module of the GENOMatch-project, meaning the **conformity of data protection collection and the management of blood and tissue samples**.

II. Object of the Survey

The object of the survey in the context of the auditing process is the CAU concept for the creation of a process of pseudonymous blood and tissue sample storage, which meets data protection and data security requirements.

This concept in the Version 2.0 from the 8th of May, 2003 was presented to the ULD for appraisal.

III. Legal Assessment of the Concept

The data protection aims from which the concept is derived will be described below (1), then the method will be explained how the process to collect and examine the samples is designed (2). In conclusion, the legal admissibility of the data protection documented process will be checked (3) along with the audit of the concept for the intended data protection management system (4).

1. Description of the Data Protection Aims

In the context of the pharmacogenetic trials, genetic as well as medical data will be collected from the trial participants or subjects. The concept assumes that a very **high need for protection** exists with both types of data. Because recognized measures and standards relating to the security context of medical data in clinical trials in the pharmaceutical industry already exist, the concept of the CAU concentrates on the protection of genetic data. The concept assumes that for genetic data, strict requirements with regard to guaranteeing data protection and data security are to be put into place when collecting data in the context of pharmacogenetic research. Vulnerabilities must be identified and, if necessary, technical and organisational measures must be developed and implemented to eliminate them.

Even in pharmacogenetics, when it is not primarily about individual gene tests rather about the valid statistical relationships between genetic data and the efficacy of a medication, the concept takes into consideration the high security value of genetic data. Because of the need of high security of genetic data, the following reasons hold true in accordance with the concept:

- The genetic make-up of a person is individual and unique.
- An individual's genetic make-up could shed light on the predisposition of that individual with regard to certain illnesses. Even if the actual onset of these diseases is caused by many other additional factors, third party knowledge of one's genetic predisposition to certain diseases can lead to grave discrimination in matters which relate to receiving employment or health insurance.
- One's knowledge with regard to the predisposition to certain illnesses can greatly influence the life of that individual, even if the onset of the disease is unknown.
- Genetic data does not only provide information to the individual whose genome has been analysed, but in addition, also provides information about his or her relatives who could also possess the same genetic predisposition.

Essentially the greatest security of personal data obtained and used in the context of research projects would be reached if this data is **anonymised**. For pharmacogenetic trials, however, the genetic and medical data cannot be anonymised even though there is no scientific interest in matching data to individual participants. The following reasons are cited for the necessity of referring to and obtaining personal data which has been collected in the context of trials:

In accordance with the German Parliament's Enquete Commission on Law and Ethics of Modern Medicine, each participant in clinical trials must have the right at any timepoint to withdraw his or her consent to participate in that trial. In such a case his or her genetic and other data must be deleted. As a result, the Enquete Commission demands being able to secure through a pseudonym process „the right of the concerned to demand a verifiable deletion or destruction of that individual's samples and other data.“

With the existing concept, the CAU is aiming for the goal of making possible the destruction or deletion of samples and other data without making it necessary for re-identification to take place at the research or storage facility where the samples are kept.

- Drug regulatory agencies have the right to demand all data up to the data record level which has been collected in the context of a trial for reviewing purposes (i.e. reviewing the accuracy of the clinical trial)
- In the context of a trial it may emerge that a participant has a genetic predisposition that is relevant for the overall integrity of his health. In order to inform the participant of this, he must be addressable.
- In the context of a trial it may emerge that certain genetic factors may cause considerable irreconcilable incompatibilities with regard to the medication being tested in the trial. In such cases the participant who possesses such a genetic make-up must be able to be notified and must be able to be excluded from participation in the trial.

Because anonymisation isn't possible, the CAU is pursuing the goal of optimal protection of processed data in the context of a trial by way of a pseudonym process. In this way it takes advantage of the fact that with scientific evaluation, an identification isn't required and a matching of genetic and medical data is enough in each case. In order to achieve the highest possible security, the pseudonym process should be designed so that:

- No individual is able to ascertain the trial or patient number of the sample donor on the basis of the attached identifiers or corresponding gene data identifiers which are found on a blood or tissue sample.
- For all participating individuals in all research projects, with the exception of the clinical trial site, the solution of the identity behind the pseudonym is only possible up to the level of the study and patient number.

2. Implementation of the Goals in the Envisioned Data Protection Concept

a) Sample Taking and Sample Analysis Method

The procedure used to collect the samples and test the samples according to the CAU concept will be described below:

The following **facilities** are involved in this process:

- Clinical Trial Site
- Central Sample Repository
- SIM Center (Secure Identity Management)
- Schering with its Secure Data Area
- Extraction Laboratory
- DNA-Analysis Laboratory

The blood or tissue samples will be taken from the patients by the Clinical Trial Site. The patients will have previously given their informed consent to participate in a pharmacogenetic study. This study will have a study number (SN). The different patient samples (n) will each be provided with a patient number (PN) along with a randomly generated 12 digit bar-code (Bar-code 1) at the Clinical Trial Site. The bar-codes belonging to one patient will be integrated into a Sample Group Number.

The Clinical Trial Site will fill out a pharmacogenetic **accompanying letter**. The original is kept at the Clinical Trial Site and a copy goes to the Central Sample Repository. The following details are contained in the accompanying letter:

- The patient number
- Information about the plausibility check which regularly depicts information obtained from the patient on a regular basis (for example, the patient's date of birth)

- The identification of the Clinical Trial Site
- The country in which the Clinical Trial Site is located
- The study number
- The confirmation of the Clinical Trial Site with regard to the receipt of the patient's informed consent form
- The label with the bar-code 1 (BC1)
- The sample's storage time limit endpoint

The bar-code is generated by the **SIM Center** (Secure Identity Management). The SIM center is accorded the status of a trust. The releasing of a study number pseudonym or patient number pseudonym can only occur through the SIM Center in the previously defined exceptional cases. Moreover, the transfer of the samples will be documented. No clinical or genetic data will be stored at the SIM center. The involvement of the Clinical Trial Site is necessary in order to identify an individual patient. This trust function shall be administered by the Datenzentrale Schleswig-Holstein.

The Clinical Trial Site will receive a number of **test tubes for the samples** from the Central Sample Repository. Two identical bar-codes 1 (BC1) will be sent together with the test tubes along with a blank label upon which the patient number is to be written. **Forms for the pharmacogenetic accompanying letter** will also be sent with each test tube. The Central Sample Repository on its part will request the bar-code from the SIM center. The investigating physician will then stick one of the BC1s together with the blank label on one of the test tubes and will stick the other BC1 on the pharmacogenetic accompanying letter, the original of which is kept at the Clinical Trial Site. The copy of the accompanying letter, which goes to the Central Sample Repository, has neither the BC1 nor the patient's name.

Finally, the labelled samples along with the copy of the accompanying letter will be forwarded to the Central Sample Repository (CSR). Within the Central Sample Repository three roles with strictly divided authority functions will be administered: the Sample Registrar, the Sample Code Exchanger and the Sample Manager. The assignment of the roles and authorities pertaining to them will be done by the CSR Administrator. The administrator himself does not have access to the CSR database tables. The *Labor für Klinische Forschung* (Laboratory for Clinical Research) in Kiel shall function as the first medically led sample repository for Schering AG.

The copy of the forwarded pharmacogenetic accompanying letter contains the following points:

- The patient number
- Information about the plausibility check which regularly depicts information obtained from the patient on a regular basis (for example, the patient's date of birth)
- The identification of the Clinical Trial Site
- The country in which the Clinical Trial Site is located
- The study number
- The confirmation from the Clinical Trial Site about the release of the patient's informed consent
- The sample's storage time limit endpoint; this information will be made available to the Central Sample Repository by the Process Controller

Three different procedures in spatially separate areas will be conducted by different employees in the Central Sample Repository:

In the first step the Sample Registrar checks the incoming blood samples or tissue samples, and then informs the SIM center about which patient number is assigned to which bar-code. He subsequently removes the patient number from the sample and stores the sample in the refrigerator (Refrigerator 1). The Sample Registrar then attaches the patient number on the **copy of the accompanying letter** and archives this.

The next step in the Central Sample Repository is carried out by the Sample Code Exchanger. This person obtains the sample from the Sample Registrar and removes the bar-code 1 from the sample and replaces this with a second bar-code (BC2) which he similarly has requested previously from the SIM Center. Finally he notifies the SIM Center which bar-code 1 is matched to which bar-code 2, and then destroys the bar-code 1 and consigns the sample which is identified with bar-code 2 to the sample manager who then places this sample in the refrigerator 2 for storage.

The pseudonym process in the SIM Center does not refer back on one uniform encrypted code. Rather, bar-codes 1 and 2 as well as the Sample Group Number will use clear and unique random numbers which will be matched to each other in a register. Thus mistakes can be avoided when creating and recognizing the bar-code. In light of the storage requirement of up to 20 years, it has to be guaranteed that during this time period, a compromising of the pseudonyms being used does not take place which cannot be guaranteed by using an electronic encoding procedure. A checking cipher will be attached to the pseudonym to safeguard against mistakes. As soon as a bar-code 2 is matched to a sample, this will be saved and the barcode 1 in the SIM Center database will be deactivated so that this can no longer be allocated out.

At the request of Schering, in the third step, the Sample Manager will forward the samples from the refrigerator 2 with the bar-code 2 either to the Extraction Lab or to the DNA Analysis Lab. The Extraction Lab as well as the Analysis Lab are institutions which are both independent of Schering. Tissue samples as well as clinical and genetic data will be analysed exclusively by Schering in the bar-code 2 pseudomised form. DNA will be extracted from the blood and tissue samples in the Extraction Lab on behalf of Schering and this will subsequently be sent back to the Sample Manager at the Central Sample Repository.

DNA sequence information will be generated from the DNA samples in the DNA Analysis Lab and these – still identified by the bar-code 2 – will be forwarded directly to the Schering pharmacogenetic data manager.

Before admitting clinical data into a pharmacogenetic trial, the data which is applicable for re-identification will be changed so that a re-identification will no longer be possible (for example, the substitution of the subject's date of birth with the subject's age). By doing this, an indirect matching of the genetic data to the patient number by way of the clinical data can be avoided. This „filtering“ belongs to the second phase of the GENOMatch-Project and is not an object of the audit.

The clinical data record contains as an identification characteristic the study number (SN) and the patient number (PN). When forwarding clinical data records to the secure data area of Schering AG (Schering Corporate Pharmacogenomics/Secure Data Area) the SN and PN will be removed (in two steps) and in their place the BC2s which belong to the corresponding patient in order to identify his genetic data will be attached. With this, another pseudonymisation step takes place. In order to avoid matching the patient number to genetic data, another additional pseudonym step of the clinical data in different areas will be conducted in two phases (Match Filter I and II). Match Filter I is found outside of the Secure Data area and replaces the PN with a Sample Group Number (SGN) via the SIM Center. The Match Filter II replaces the SGN with the BC2.

Genetic and medical data are compared and analysed at Schering with bio-statistical methods. The genetic data available at Schering are also barc-code 2 labelled.

The scientific evaluation of the clinical and genetic data will take place in the Secure Data Area of Schering AG. Only aggregated data – not single data records – are allowed to leave this area. A genetic and a clinical database will be conducted in this area. The genetic database contains genetic data generated from the DNA Analysis Lab (long-term storage). The clinical database contains the pseudonym and filtered patient data from the clinical trial. The clinical data will be deleted after the end of the pharmacogenetic trial. Access to the area will be separately controlled. The Net access to the data in this area is secured by a firewall.

The medical data will be kept at Schering AG as long as it is needed for the comparison and for the bio-statistical evaluation. The scientific evaluation will take place in the Schering Corporate Pharmacogenomics/Secure Data Area. In addition, Schering takes the full responsibility for the process and implementation of the data protection concept. The long-term storage of the genetic data and the short-term storage of the filtered clinical data will take place in the Secure Data Area. For the analysis (i.e. the matching of the genetic and clinical data) it is also conceivable that both BC2 identified data records are transferred to an external location with a Secure Data Area which will also have to show that it operates according to Schering standards.

The following people/roles will operate within the Secure Data Area: The Administrator will assign the user roles, to which at least one representative will be assigned. The Process Controller will monitor the workflow in the whole GENOMatch-process including the handling of the data and the samples at the authorized facilities and will conduct the internal audit. He has the complete responsibility over the GENOMatch process. The Pharmacogenetic Data Manager is in charge of the correct filtering of the clinical data as well as the security function of the IT system at Schering. The Pharmacogenetic Biostatistical Expert will define the genetic data set to be generated for each analysis project.

It is also conceivable that the scientific evaluation of the clinical and genetic data will be assigned to an external Pharmacogenetic Data Analysis Facility. In this case, the BC2 identified clinical and genetic data records will be turned over to this facility. The external facility must likewise operate a secure data area in accordance with the standards established by Schering. Furthermore, Schering will be held completely responsible for the process and the implementation of the data protection concept.

During the whole process, the SIM Center will be accorded the task of generating pseudonyms like the bar-code 1 and bar-code 2 as well as the Sample Group Number. In addition, the SIM Center will have access to a data pool which results in the **matching of the sample pseudonyms** bar-code 1 and 2 **and Sample Group Number** to each other and to the **Study Number** and the **Patient Number**. The SIM Center does not have access to the patient names. This information is known only by the Clinical Trial Site.

The samples will be stored in accordance with the informed consent for up to 20 years and thereafter will be destroyed. Shorter **storage times** are possible according to this concept.

To **ensure the quality** of the sample storage and the analysis procedure, non-human tissue/blood samples (i.e from apes) will be brought into the Central Sample Repository from the Clinical Trial Site at irregular intervals.

b) Procedure in the Case of Revocation of Patient's Consent

In the case of the revocation of a patient's informed consent to continued participation in a trial, the concept envisions the following procedure:

The patient's withdrawal of his consent to participate in a trial is given to the trial investigator or to the Clinical Trial Site. The investigator then informs the responsible Sample Registrar at the Central Sample Repository in writing about the revocation of consent. The **trial and patient number specifications as well as the specifications to check plausibility** (patient's date of birth) are included in this information. The name of the patient may not be disclosed when doing this. The Sample Registrar then sends a request to the SIM Center which matches the trial and patient number to the bar-code 1. In addition, the request contains the study and patient number along with the specifications of the plausibility check. In order to avoid fraudulent inquiries, the SIM Center will send a copy back to the Schering Process Controller.

If a bar-code 2 hasn't yet been attached to the patient's sample, then the SIM Center informs the Sample Registrar of this by an encoded and signed e-mail stating which **bar-code 1** had been assigned to the patient. The Sample Registrar then destroys the sample with this bar-code 1. If a **bar-code 2** has already been assigned, the SIM Center will inform the Sample Manager of this and the corresponding sample will then be taken out of refrigerator 2 and **destroyed**.

Simultaneously via an encrypted and signed e-mail the following parties will be informed:

- The extraction lab or the DNA Analysis Lab, in case the samples have already been forwarded to them. These facilities will then subsequently destroy the samples and delete, if already transferred, the genetic data. These facilities will subsequently confirm this to the Sample Manager, who will then update the sample status.
- Schering, in case the data has already been generated. This data will then be deleted by the pharmacological biostatistic experts and the deletion will be confirmed to the SIM Center.

As soon as a destruction or deletion of samples or data is confirmed at the SIM Center, the SIM Center will then inform the Sample Registrar about the deletion of a specific patient number. The Sample Registrar then **confirms the destruction/deletion** with a signature on the **copy of the accompanying letter** and conveys the information about the destruction/deletion to the investigator or Clinical Trial Site. The investigator or Clinical Trial Site will then archive the documentation together with the revocation of the patient's informed consent along with the other documentation regarding the patient's earlier participation in the trial.

3. Legal Basis for the Legitimacy of the Data Security Procedure

The admissibility of the conduct of pharmacogenetic trials and the storage of tissue samples used in them is based on the **informed consent** of those concerned.

The process of obtaining this consent is not the object of the existing audit. This audit is concerned with the legal basis of additional secure data processing after legitimate collection of data by the Clinical Trial Site. It is important to bear in mind that tissue samples and genetic data used for scientific trial purposes are to be handled as confidential patient information (§ 203 StGB, § 9 MBO-ÄK). In this sense these details deal with health and certain types of personally derived data as pertains to § 3 section 9 of the BDSG. According to § 28 section 6 of the BDSG the processing of such information is admissible in the context of the informed patient consent pertaining to § 4a section 3 of the BDSG. If third parties, other than those stated persons, receive legitimate knowledge of health related information, then these parties are obliged to heed the same laws that apply to an investigator.

The processing procedures at the SIM Center, the Central Sample Repository as well as those of the labs designated as **data processors on behalf** of Schering each are to be classified from a data protection point of view as legitimate pertaining to § 11 BDSG. All the processes are carried out in pseudonym form in order that the transfer of samples, evaluation results and accompanying letters do not reveal any confidential patient information. The instructions with regard to the contractors have been generally established in written form in the concept as well as in the corresponding contracts. In doing so, individual case deviations are to be eliminated.

According to § 9 of the BDSG, it is expected from the responsible party as well as those contracted parties which process data, to meet the technical organizational criteria which are essential in the legal requirements as well as those stated goals appended to this regulation. Included in those goals is preventing the access of unauthorized parties to confidential personal data as well as guaranteeing the authenticity and the accessibility of this data. (Numbers 1,3,5 & 7 annex to § 9S 1 BDSG).

According to § 3a of the BDSG the design and selection of a data processing system is to be configured in such a way that no personally derived data or as little as possible personally derived data is processed (Policy of Data Avoidance and Data Economy). As far as possible, it is especially desirable to use an anonymisation or pseudonym process if the effort of doing so is reasonable in relation to the desired data security.

These regulations of the BDSG comply with the legal requirements of the 95/46/EU Directive of the European Parliament and of the council of 24 October 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data. (European Data Protection Guideline – EU- DPGL, esp Article 2 lit. h, Article 8 section 1, Article 17 EU-DPGL). They go above and beyond § 3a BDSG.

Article 14 of the revised framework guideline for the International Declaration for Human Genetic Data of the International Bioethics Committee of the UNESCO envisions that for scientific purposes collected data must be separated from an identifiable individual. If this division is rescindable, precautions must be taken to ensure the confidentiality of the data.

The double pseudonym process that is envisioned in the concept guarantees the implementation of the requirements of the §§ 3a, 9 BDSG and the above mentioned guidelines. It takes into account the high sensitivity and protection value of the stored tissue or clinical and/or genetic data. With pseudonyms, it can be avoided that authorities acquire the identity of the trial subject in the context of pharmaceutical inspections.

The concept aims to safeguard the confidentiality of data from external and internal attacks. Protection from internal attacks is achieved by role based access control. Attempts at abuse during data processing will be logged and recorded. The register in the SIM Center will be filed in an encoded manner. A firewall system will be installed to protect against unauthorized Net attempts at accessing the system. The communication between the SIM Center and the Central Sample Repository will take place in an encrypted fashion through a Net tunnel so that eavesdropping by unauthorized parties can be excluded.

The concept also ensures in isolated cases when informed consent is withdrawn after a successful pseudonym process, that a deletion of the data or a destruction of the samples can take place and that any requests for information from the concerned parties or any notification of the concerned can still be satisfied. At the same time it can also be guaranteed that the trial subject remains anonymous to those participating in the research project during the complete scientific processing of the samples and the data by way of the secure double pseudonym procedure. Even in the case that genetic or clinical data fall into the hands of an unauthorized party, the activation of the matching procedure requires two separate and independent sites.

Not only the existing legal basis of the data security requirements will be implemented by realization of the concept. In fact, technical standards will be set which also will, in the medium-term, satisfy the increasing requirements of the security of genetic data. The normative conditions for the handling of genetic material or genetic data will be met, corresponding to the current preliminary legislative debate (see Final Report of the Enquete Commission „Law and Ethics of Modern Medicine“ from 14 May 2002, BT-Drs. 14/9020, Chapters 2.2.2.6 & 2.4).

In light of the high data security standard when using the pseudonym process, the storage time of up to 20 years can be considered maintainable.

4. Data Protection Management System

Because complete patient related identification features are stored in the SIM Center database, its technical structure is of vital importance for the the whole GENOMatch infrastructure. The SIM Center has four functional components: the SIM Center database, the Identity Management – IM application, the Sample Tracking – ST application and the Audit application. The IM application has exclusive access to the pseudonym registers, the ST application has access only to the information regarding the sample status and the Audit application has access only to the protocol data. In this way, no one part of the SIM Center has access to the whole of a pseudonym stored data pool.

The **database** contains, in addition to the IM, the ST and the log registers, tables for guaranteeing role based access to the data base. The IM table area is encoded. A quality control of the incoming samples and sample identification will be undertaken at the Sample Registrar. The reasons for any irregularities will be stated in an audit trail and will lead either to a correction or the destruction of the samples.

For the purpose of conducting checks the authorized data protection commissioner of the SIM-Center and – if required – the responsible data/privacy protection authority obtain access to recorded data on the role based authorized access tables as well as to the patient numbers (but not to the bar-codes or Sample Group Numbers). A checking of the copies of the accompanying letters is also possible in order to more effectively check the existance of consent forms.

The whole data exchange between the SIM Center and the communication partners is encoded through an SSL-Tunnel. By way of the SSL-Tunnel, a secure user authentication is simultaneously achieved. The authentication should then follow with a chip card based signature procedure. The access to the chip card will be safeguarded by using a PIN.

The SIM Center is protected by a firewall system. Only HTTPS inquiries from the Central Sample Repository via a defined port as well as SMTP inquiries from or to the Central Sample Repository will be exclusively allowed. In and outgoing e-mails will be checked for viruses and, in the case of a virus, isolated. Active contents will not be admitted.

In order to avoid a compromising of the matching tables (with SN, PN, bar-codes, SGN) via an infiltrated sniffing program, the complete workstation computers in the Central Sample Repository will be operated as Thin Clients upon which users will not be able to install any further software in addition to the Internet browser. Chip card readers are envisioned for authentication purposes.

Schering Corporate Pharmacogenetics (CPG) Manager is responsible within Schering for the correct process and handling of the data. He assigns authorization in accordance with the roles for a defined period of time. The same is true for the Central Sample Repository. The granting of rights is to be carried out by each administrator.

The **data protection concept** will become a part of the documented Standard Operating Procedure. All of the affected employees have to familiarize themselves with this data protection concept.

The Schering Process Controller **monitors** at regular intervals the user log. If irregularities are discerned, the CPG Manager is to be immediately informed.

Complaints by trial subjects will be conveyed via each clinical trial site in order to avoid Schering obtaining knowledge of the identity of the subject in question.

The **authorized company data protection commissioner** of Schering will be regularly called upon to check the GENOMatch-IT-Infrastructure.

A **Pharmacogenetic Advisory Board – PGAB** will be set up as an independent control and advisory body with external experts from the fields of pharmacogenetics, bio-science, ethics and law. The board must agree to the general protocol of each trial. A veto from the board can only be overruled by the Schering AG board member responsible for Research and Development.

5. Cumulative Appraisal

The existing concept of the CAU for a data processing structure for secure pseudonym storage and safekeeping of blood and tissue samples for genetic analysis usage fulfills the legal requirements of **data protection** and **data security**. The envisioned pseudonym process guarantees a standard of security which goes beyond the previous methods and which sets a new benchmark. The presented **data protection management system** also ensures a long-term preservation of the data security.

The coherent and comprehensive concept is well qualified for upholding the **trust of trial subjects** with regard to the long term safekeeping of personally derived data in the context of a pharmacogenetic medical research.

The bestowal of the **data protection audit** in accordance with § 43 Sec. 2 LDSG is herewith justifiable.

Unabhängiges Landeszentrum für Datenschutz
Independent State Centre for Privacy Protection
Schleswig-Holstein
Holstenstraße 98 / 24103 Kiel
Telephone: 0431/988-1200 Telefax: 0431/988-1223
E-mail: mail@datenschutzzentrum.de
Homepage: <http://www.datenschutzzentrum.de>