Title: METHOD AND SYSTEM FOR THE ANALYSIS OF MEDICAL AND PERSONAL DATA

Abstract: The patent application relates to a method and system for the analysis of medical and/or personal data. Exemplary embodiments disclosed in the application include anonymously questioning customers about their lifestyle and their reactions to various drugs, thereby offering the opportunity to identify new indications and modify current formulations of drugs. A further exemplary embodiment enables a manufacturer or provider of services to strengthen the relationship with existing customers by providing rewards to the customer. In addition, this patent application describes specifically and in general personal information systems, health care systems and systems for the administration of diagnostic and genetic tests. Exemplary embodiments disclosed herein relate to user-oriented health management and individualized diagnostics and therapeutics. Other embodiments provide methods and systems for substantially or completely anonymously administering a test - particularly a genetic, diagnostic, or physical test - on one or more users; and methods and systems for enabling a user to make personal health risk assessment in a substantially secured manner.
Method and System for the Analysis of Medical and Personal Data

Summary of the Invention

The disclosure relates to a method and system for the analysis of medical and/or other personal data. The method and system disclosed herein can be used for a variety of purposes and is not necessarily limited to the embodiments related to medical data. Exemplary embodiments disclosed herein include anonymously questioning customers about their lifestyle and their reactions to various drugs, thereby offering the opportunity to identify new indications and modify current formulations of drugs. A further exemplary embodiment enables a manufacturer or provider of services to strengthen the relationship with existing customers by providing rewards to the customer.

In addition, this disclosure describes specifically and in general personal information systems, health care systems and systems for the administration of diagnostic and genetic tests. Exemplary embodiments disclosed herein relate to user-oriented health management and individualized diagnostics and therapeutics. Other embodiments provide methods and systems for substantially or completely anonymously administering a test – particularly a genetic, diagnostic, or physical test – on one or more users; and methods and systems for enabling a user to make personal health risk assessment in a substantially secured manner.

Prior Art

The completion of the working draft of human genome sequence has marked a significant milestone in man’s everlasting endeavor to decode life. It is estimated that the total number of expressed genes or transcription units in a human genome is around 30,000 – 40,000 (Venter G. et al., Science 2000, Vol., 291: 1304-1351; The Genome International Sequencing Consortium, Nature 2000, Vol. 409: 860-921). The number of human proteins is expected to significantly exceed this estimate because, in many cases, more than one RNA splice variant is transcribed from a transcription unit or a gene. Estimates vary, but some researchers believe that there exist up to 500,000
human RNA transcripts and that, more than 30% of genes or transcription units in the human genome produce several RNA splice variants. (Mironov et al. 1999, Genome Research 9:1288-1293). Considering further the individual genomic diversities in the human species, evidenced, for example, by an increasing number of single nucleotide polymorphisms ("SNPs") identified, this immense genomic data pool lays the foundation for a better understanding of human physiology and brings about significant therapeutic and diagnostic promises.

Of particular relevance is individual genetic predisposition, a challenging area to biomedical researchers, genetic counselors, as well as clinicians. It is estimated that the DNA sequence of any two given human beings differ by approximately 0.1%. These differences in DNA base composition can result in different protein functions, and thus become consequential with respect to the individual’s physical well-being in some situations.

Recent years have seen dramatic growth in the information of genetic predisposition, the responsible genes, and their specific mutations. More mutations are being detected which are connected to higher risks of developing certain diseases, often with an earlier onset. For example, there are an increased total number of entries in the Mendelian Inheritance in Man (which has more than 10,000 entries as to date). See also, the Online Mendelian Inheritance in Man database (OMIM) at http://www3.ncbi.nlm.nih.gov/Omim/searchomim.html. As consequences of genetic predispositions are better appreciated today, techniques for genetic diagnosis are made available in clinical settings. An increasing number of genetic tests are offered to measure the potential mutations. As of 1999, 667 different genetic tests (excluding DNA-analysis tests for infectious diseases) were offered, up from 111 in 1993 (GeneTests.org, Washington G2-Reports: Lab Industry Outlook 2000 as cited in Merrill Lynch, In Vitro Diagnostics, 14 November 2000).

Whereas advances are being made to find cures for some genetic diseases, many of them do not yet have effective therapies. However, lifestyle and dietary avoidance strategies are becoming feasible for a significant number of genetic diseases, which makes it extremely critical and beneficial to detect genetic predispositions early in time. That is, if an individual knows that a disease-
responsible gene – a gene that is involved in the development, onset, or progression of a disease – carry mutations in his or her genome, he or she may institute recommended changes in lifestyle and diet to postpone or avoid the outbreak of the disease. Therefore, the diagnostic and therapeutic promises of the human genome data may be realized as the data is transformed into personalized knowledge on individual genes and their impact on the onset and severity of a disease.

Predisposition to adverse drug response is similarly of importance. Adverse drug reaction is one of the leading causes of death in hospitalized patients worldwide. It is recognized as the fourth to fifth leading cause of death in hospitalized patients in the United States. Of more than two million Americans hospitalized each year for adverse drug reactions, over 100,000 people die (JAMA 79, 1200–1205 (1998)). Genetic predisposition testing is rather promising in potentially eliminating these deaths because heritability (or the genetic component) plays a large part in adverse drug response. Prediction of drug response therefore would have profound impact on the delivery of personalized therapeutics; a goal sets out by the new evolving discipline, pharmacogenomics.

In sum, there is a huge and increasing demand for genetic tests – or other diagnostic and physical tests, for that matter – propelled by the new genomic knowledge and technology capacities, as well as individuals’ desire to be better self-informed of health risks and their desire to engage in proactive personal health management. A recent poll in the U.S. and Europe indicate that approximately 2/3 of all people in western societies would like to know their genes and their genetic predisposition.

There is moreover a need to identify and correlate adverse drug reaction with the genotype of the individual taking the drug. This can often only be established by undertaking large-scale studies of patients. There is therefore the need for establishing a system and method for noting the drugs taken by a patient or test subject and for recording the patient’s genetic disposition and for correlating the data. Large-scale studies have to be carried out in order to identify the causes for the adverse drug reaction.
However, to meet such demand and to empower individuals to engage in proactive personal health management, certain issues must be addressed, including especially the issue of privacy. People generally fear that genetic information may be made available to third parties – such as employers and insurers – and used to their detriment. In order to address this concern, an appropriate or reasonable level of privacy must be ensured, advantageously including high-standard security and anonymity.

One example of such a genetic test is known from PCT Patent Application No. WO 00/28460 (Maus et al.), assigned to Lifestream Technologies, Inc. This application discloses a health monitoring and diagnostic device with a network-based health assessment and medical records maintenance system. The monitoring and diagnostic device is a hand-held meter that includes an enclosure for housing a disposable test strip for use with the meter. Within the meter, a processor is included that is functionally connected to a reader for the disposable test strip as well as to a user input device and a display device. The processor contains a program module that obtains the test results from the test strip reader and causes the display device to display the test results. A data drive writes the test results to a removable memory storage device, such as a smart card.

The Maus et al. PCT application furthermore describes a secure medical records maintenance system that is specifically adapted for use with the health monitoring and diagnostic device. The maintenance system may store any type of electronic data, including a wide variety of medical records, for example electronic medical data generated remotely from the hospital or doctor’s office environment. The maintenance system further includes a number of removable memory storage devices. Each removal memory storage device also stores a patient-specified personal identification number (PIN), a medical records identification number and a patient identification number, both of which are secured by the PIN.

The data on the removable memory storage device is downloadable to a two-server system. The first remote server of the two-server system stores patent identification information indexed by patient identification numbers. The second remote server of the two-server system stores patient medical data indexed by the
medical records identification number. For security purposes, the medical data maintained in the second remote server cannot be correlated to the associated patient identification information maintained in the first remote server.

To allow correlation of the data stored in the two servers, the secure medical records maintenance system includes a correlation table uniquely associating each medical records identification number with a particular one of the patient identification numbers. The correlation table for a particular patient resides on the patient’s removable memory storage device. According to the application, the correlation table may also reside on the practitioner’s computer.

According to this patent application, the patient’s medical practitioner supplies the patient with a health monitoring and diagnostic device. The medical practitioner enters data relating to a new patient through an interface connected to the Internet and the software associated with the secure medical records maintenance system assigns a unique patient identification number and a unique medical records identification number. The means for payment for the test can either be made through the medical practitioner or by the patient himself or herself, for example by means of a debit or credit card.

The secure medical records maintenance system of this application requires the patient to be supplied with the appropriate health monitoring and diagnostic device before the test is ordered. Analysis of the test results is carried out either at home or in the medical practitioner’s surgery and the results transmitted over the Internet. As the medical practitioner is responsible for initially activating the system, the results of the tests on the patient are available to the medical practitioner and the patient’s data is therefore not anonymous. As a result of the intervention of the medical practitioner, the patient cannot order a test without the knowledge of the medical practitioner and also tests cannot be ordered for other people. Finally, the correlation between the patient’s identification number and the medical records identification number either on the smart card or in the doctor’s surgery means that, under certain circumstances, the patient’s data may be accessible to unauthorised parties in possession of the correlation.
PCT Patent Application No WO 01/65443 (Demopulos) also teaches a method and a system for registering the results of a medical test on a subscriber (test subject) in which the results are only accessible to authorised parties over a communication network, such as the internet. The system receives the results of the test from a testing agency together with details allowing the identification of the subscriber and stores these results in a registry. Access to the registry is enabled to the subscriber and any party authorised by the subscriber.

The object of the Demopulos application is to provide a registry accessible over the Internet for the storage and access by the subscriber, person tested and/or authorised medical personnel. The primary purpose of the service described in this application is to enable proof of a medical condition that can be presented to a sexual partner. Thus the results of the medical tests will be correlated with the identity of an individual and may therefore be potentially accessible to unauthorised parties.

Finally, PCT Patent Application No. WO 01/69430 (Rienhoff et a.) assigned to DNA Sciences, Inc., teaches a secured database which is populated with genotypic and phenotypic data. The server is coupled with a worldwide network of computers and provides a web site that is configured to create trust of the web site by the users. Users are invited to submit phenotypic data and a biological sample. The secured database is populated with the received phenotypic data, and the received biological samples are analyzed to obtain genetic data.

Users are encouraged to trust the web site and thus provide information by several means. For example, the web site is configured to restrict access to the data. The user is also provided with reliable and valuable information regarding genetics, diseases, medical conditions and the like. A support framework within the web site can also be established to increase the trust and also a referral service can be provided.

Notwithstanding these features, unauthorized access to the database would allow the correlation of data between the identity of the patient and the provided phenotypic data and biological sample.

Summary of the Invention
To meet the demand for genetic tests and to empower individuals to engage in proactive personal health management, issues of privacy and restricted access to the results of the medical tests must be addressed, as discussed above. Potential test subjects generally fear that the results of the tests and the genetic information obtained may be made available to third parties - such as employers and insurers - and used to their detriment. In order to address this concern, an appropriate or reasonable level of privacy must be ensured. This should advantageously include a high standard of security and anonymity.

These and other objects of the invention are solved by providing a method for anonymously administering at least one test for one or more test subjects which comprises the following steps:

In a first step, an orderer, i.e. a person who orders the test, records in a first repository his or her identity data. The orderer can be, but is not necessarily, identical with the test subject, i.e. the person on whom the test will be performed.

In a second step, a kit is forwarded to each of the orderers without referencing the identity data of the test subjects. The kit comprises instructions on the test and materials for taking a sample for said test.

In a third step, the sample is received from the test subject and in a fourth step a result is obtained from the sample for the test. This result is recorded in a second repository under a unique identification code. The first repository and the second repository are insulated from each other, i.e. it is not possible to correlate the data in one repository by reference to the data in the other repository.

By means of this method, the identity data of the orderer of the test and the test subject are kept separate from the results of the test. Thus anonymity of the results of the test is assured, since it is not possible to trace the test subject from the stored results. Even in the event of a computer error or hacker attack, the results of the test cannot be correlated with the identity of the orderer of the test or the test subject since the first and second repositories are different from each other. Unlike in the prior art, no correlation table is provided which allows a connection between the identity of the orderer and the results of the test on the test subject.
The method of the invention also has the advantage that it allows the orderer of the test to be different from the test subject. In addition, ordering of the test can be carried out through the Internet or over the telephone without the intervention of a further person, such as a hospital, pharmacist or medical practitioner. Furthermore, the test can be purchased anonymously from a pharmacy.

A further degree of security is provided by a method in which the unique identification code is created by the orderers without reference to any pre-assigned identification codes. The orderer of the test can thus only know the identification code.

The method has been used for providing a diagnostic test for a disorder, such as coagulation and thrombosis disorders, hemochromatosis, cancer, and HIV. The method could also be used for a genetic test for one or more genotypical or phenotypical traits. This list of tests is not limiting of the invention. The list indicates those tests in which concern has been expressed about the anonymity of the test subjects and the risk that the results could get into unauthorised hands.

In a further embodiment of the invention, each of said test subjects can create a unique password that corresponds to the unique identification code. The unique password allows the test subject to access the result of the test stored under the unique identification code (and without reference to the test subject’s identity) in the second repository using the unique password. This provides an additional layer of security for accessing the results of the test.

The object of the invention is furthermore solved by providing a system for anonymously administering at least one test for one or more test subjects. The system has a first repository in which the identity data of an orderer of the test are stored. The orderer, on registration to the system, provides the identity data to allow delivery of the kit and payment for carrying out the test. The system further includes a kit comprising instructions on carrying out the test and materials for taking a sample for the test. The kit is forwarded to the test subjects with a unique identification code. This unique identification code is preferably supplied in a “hidden” manner in which the unique identification code is initially concealed by an adhesive label that is removed either by the orderer of the test or the test subject. The adhesive layer is
preferably made from a plurality of layers for security purposes. An attempt to remove the adhesive layer will lead to at least partial destruction of at least one of the plurality of layers and will thus indicate to the recipient of the kit that the kit has been tampered with.

The results are only accessible to the test subject on receipt of the unique identification code and, if enabled, receipt of the password.. The first repository and the second repository are insulated from each other, as explained above.

The system includes a first interface that is capable of receiving the identity data entered by the orderer upon registration. The first interface connects to the first repository and provides the identity data to the first repository for storage therein. In one embodiment of the invention, the first interface comprises a first data transfer system for transferring the identity data to an intermediate storage and a second data transfer system for transferring the identity data from the intermediate storage to a local storage. This embodiment has the advantage that an additional layer of security is provided since the first interface and the local storage are not directly connected to each other.

The system also includes optionally a second interface with a password storage area. The second interface is capable of providing the result of the test stored under the unique identification code when the unique password is entered by one of the test subjects. The second interface is connected to the second repository for accessing the results of the test. Only if the entered password corresponds to the unique identification code will the medical and/or personal data be provided to the test subject.

In a further implementation of the invention, the system can be supplied with a third repository connectable to the second repository for studying the health conditions of the test subject and/or assessing the health risks of the test subject. This third repository can be a knowledge base or expert system that analyses the medical and personal data and provides the test subject with more detailed information.

In yet a further implementation of the system a fourth repository is provided. The fourth repository stores, upon receipt of an instruction from each of the test
subjects, said sample or biological molecules derived from the sample for a specified period of time. This allows the sample to be retested, if required.

A further embodiment of the invention provides for a classification schema stored in the third repository and based on said test. Using this classification schema the test subject and assess his or her personal health risks. Advantageously the classification schema lists a plurality of risk classes ranked from lowest risk to highest risk, the risks being relating to said one or more health disorders.

In the system, a computer-readable medium is provided on which is stored a data structure. The data structure has one or more first fields containing medical and/or personal data representing results of the tests and a second field containing a unique identification code permitting access by the test subject to the medical and/or personal data in the first fields. A third field with the unique password created and supplied by the test subject can also be stored in the data structure on the computer-readable medium.

As discussed above, there is also a need to allow access to the collected medical and personal data for analysis in order to determine, for example, side effects or to correlate interactions between a test subjects genotype and phenotype.

This object of the invention is solved by providing a method for the analysis of medical and personal data that has the following steps. In a first step, at least one item of medical and personal data is obtained from the test subject. This item of medical or personal data is recorded in a second repository under a unique identification code. To analyse the medical and/or personal data, it is extracted from the second repository and a conclusion reported. The conclusion report could involve, for example, the analysis of the medical and personal data to determine side effects or the correlation of more than one item of medical and/or personal data to determine significant, as yet undiscovered, information, e.g. on the phenotypes of individuals. This will allow the development of better formulations related to the genotypes of the information and also result in new indications of existing drugs. Collecting this medical and personal data will allow a systematic analysis of the medical and personal data, thereby enabling faster and more accurate analysis. In the past, discovery of new indications
of known drugs, such as the effect of sildenafil citrate on erectile dysfunction has relied on observational skills.

The advantage of anonymously recording the medical and personal data is that test subjects, in particular human beings, are more liable to provide the medical and personal data if they are assured that there can be no access to the medical and personal data identifying them as the provider of the medical and personal data.

Items of medical or personal data recorded in the depository include, for example, information obtained from a test laboratory to which the test subject has provided a biological sample. Such a biological sample is obtained from the test subject using a test kit. This test kit can be ordered either by the test subject him or herself or it could be obtained by another person or orderer. Allowing another person to order the kit further ensures the anonymity of the test subject providing the medical and personal data, since the identity of the test subject can never be established. It is, of course, possible but not required for the test subject to be identical with the orderer.

The method is not only applicable to the recordal of medical data and personal data related to medical problems, but can additionally be used to anonymously record personal data for use by manufacturers of other products and service providers to question their customers and thereby strengthen the relationship to the customers. This could occur, for example, when a new product is launched and the seller or the product wishes to establish the acceptance of the product in the marketplace. More generally, the method is applicable to any product or service in which the customer needs to be provided with an incentive.

Additionally, opinion research institutes can use the method to survey a the opinions of members of the public and thereby reward them for their time.

Another supplier of the test kit could be an information seeker who is looking for medical and/or personal data. Such an information seeker could include an academic researcher who is carrying out, for example, large-scale studies of phenotypes of the population and requires access to large amounts of medical and personal data. The academic would supply potential test subjects with the test kit. The test subject would then forward the biological samples taken to a laboratory for
further analysis. The information seeker could also be a pharmaceutical company interested in understanding the effects of particular drugs on test subjects. In the latter case, the information seeker might well be interested in recording medical data such as side effects, genetic data and/or the lot number of a medical or pharmaceutical product. Recordal of side effects and genetic data allows investigation of the dependence of the pharmaceutical on the genotype of the test subject. Recordal of the lot number will allow, for example, quality control of the pharmaceutical product.

The information seeker may also be interested in recording information about other products such as orthopaedic products.

In one advantageous embodiment of the invention, the medical data recorded includes a pointer to a sample store in which the biological sample has been stored. This allows later re-testing of the biological sample to obtain further data or check the accuracy of the original medical data.

One embodiment of the invention includes a step of storing the identity data relating to the test subject in a first repository insulated from the second repository. In this context, “insulated” means that no correlation is possible between the medical and personal data in the second repository and identity data in the first repository. This ensures that the medical and personal data remains confidential, as there is no possibility of correlation between the medical and personal data and the identity data.

One advantage of storing the identity data is allow the information seeker to question the test subjects about their medical condition. The identity data can also be used to reward the test subjects for supplying the at least one item of medical or personal data. Such rewards might, for example, be in the form of a cash card, telephone card or other vouchers or incentives which can only be used after entry of an authorization code.

The ability to reward test subjects is particularly advantageous in establishing a long-term relationship with the customer and other potential purchasers of a drug. The customer can be rewarded for purchase of multiple quantities of the product without his or her identity being revealed to the manufacturer or retailer of the product.
A test subject can also be encourage to participate in questionnaires and other studies on the influence of, for example, lifestyles and/or the environment on the test subject’s health. In this case the test kit supplied to the test subject may consist merely of a questionnaire and a reward card. On return of the questionnaire, the test subject is provided with an authorization code to enable the reward card to be used.

The object of the invention is also solved by providing a system for analysis of medical and personal data having a first repository for the storage of identity data and a second repository for the storage of at least one item of medical or personal data. As explained above, the second repository is isolated from the first repository. Finally the system also includes a data analyser connected to the second repository and isolated from the first repository. The data analyser analyses the medical and personal data and can report conclusions from the data analysis.

**Brief Description of the Drawings**

Fig. 1 depicts a computer system for anonymously administering one or more tests and for enabling personalized health risk assessment according to one embodiment of disclosure.

Fig. 2 depicts a flow diagram illustrating the method for anonymously administering one or more tests.

Fig. 3 depicts an encrypted e-mail as sent over the network with the details of the order.

**Detailed Description of the Embodiments.**

**Privacy, Security And Anonymity**

A feature of certain embodiments of the methods and systems of the present disclosure is a reasonable level of privacy. Such a level of privacy is achieved by instituting predetermined levels of security and anonymity in the involved structural components and dynamic processes, thereby enabling users to perform one or more
tests of interest, establish and manage personal health profiles, make health risk assessments, and seek further medical counseling as needed.

The test results are stored into a repository, also referred to as a databank; it is preferably an electronic repository such as a database. Analogized to a Swiss bank, the databank is highly secured, having completely anonymous electronic accounts for the user. A user defines or is assigned his own unique password that is known only to the user and not accessible to any third party, including the data bank operator. While a password generally will be the easiest method for a user to identify himself or herself, it is expressly understood and contemplated that the skilled artisan could substitute for a password other possible user recognition hardware, software, methods and/or systems, including for example, user IDs, biometric and behavioral recognition systems such as fingerprint, voice, face, retina and signature recognition systems, smartcards, badges, and other electronic and digital signature systems, to name only a few. Likewise, combinations of the foregoing could be used. Hence, unless indicated to the contrary, a reference to the use of a password in this disclosure is understood to include by reference the interchangeable use of one or more of any such means of recognition.

In the embodiments disclosed herein, encryption can be implemented for data transfer into and out of the databank. The databank of such embodiments thus can be reasonably highly safeguarded against user-identity hacking. In extremely unlikely cases where hackers break into the databank, the identities of the users will still remain inaccessible if there is substantial or complete anonymity of the databank. Thus, embodiments disclosed herein can provide users with a reasonable level of privacy especially if a high level of security is coupled with a high level of anonymity.

In a variant of this embodiment, the databank can store medical data (such as genetic data) or other personal data for a user, which data he or she has obtained from other sources. For example, the user may have some test results from earlier tests performed in other places or contexts, and these results can be transferred by the user to the databank and stored within his or her record under the unique identification code.
Examples of further medical data that can be stored in the databank include medical data concerning the drugs, which are taken by the user, and side effects recorded by the user when taking said drugs. Data about other products, such as orthopedic products can also be stored. An information seeker, such as a pharmaceutical company or an academic researcher, carrying out a study and who is interested in monitoring the effectiveness of drugs or correlating the side effects of drugs with genetic data can specify further medical or personal data which should be recorded in order to allow the information seeker to draw conclusions from the study.

Additional repositories can be employed in other embodiments to store and manage other pertinent information, including, inter alia, users’ personal information, their family history and medical history, general medical background information on specific disorders or abnormal conditions, and information on the related diagnostics and therapies. These repositories may be implemented with lower or higher privacy level (typically lower) as desired. For example, in a particular embodiment, a first repository is used which has stored therein the user identity information. In this embodiment, the aforementioned databank is then referred to as the second repository. In contrast to the second repository, the first repository does not require anonymity or strict security measures. Rather, its main objective is to keep track of the users, and permit users to as they register with the system and order the necessary sampling kit for one or more genetic or diagnostic tests.

The first repository can also be used to follow-up the users of the system. For example, an information seeker may wish to send out questionnaires to the users on various health matters. It is also possible that an information seeker may wish to reward users for supplying medical and personal data to the databank. In order to do this, access to the identity data in the first repository is required. Given that the databank (second repository) is insulated from the first repository, it will not be possible for the information seeker to identify whether the user has actually supplied the medical or personal data, but the information seeker will be in a position to question the users.

In another embodiment, and as a further example, a third repository can be employed which is a medical knowledge base. This third repository can include, for
example, general biomedical background information on human physiology, diseases, diagnosis and therapies, information on users' medical history, information on medical practitioners and specialists, among other things. The third repository, as all the other repositories employed according to this disclosure, is preferably a database and linked to an interface through which the user may input instructions such as search queries and view the output results. In one embodiment, on his or her own command, a user may choose to transfer his or her test results, which is stored at the first instance in the aforementioned databank in an absolute anonymous and secured fashion, to the third repository, thereby allowing more extensive analysis and/or counseling on his or her health conditions. Such further analysis and/or counseling may be sought, for example, from a medical practitioner having certain special expertise of interest, identified by the user from the information presented by the third repository. The counseling may include advice on new medication, avoidance of certain drugs, specific diets and life style recommendations, for example. Alternatively, such further analysis and counseling may be obtained as the user queries the third repository through the interface and reviews pertinent information retrieved therefrom. Depending upon its purpose and function, the third repository can operate with different levels of privacy or even no privacy, and may not require the same level of security and/or anonymity as the second repository, i.e., the databank, which normally has high security and/or anonymity.

Yet other embodiments employ a fourth repository that has stored therein the biological samples from the users, or any biological molecules such as DNAs, RNAs, and proteins extracted therefrom. In one embodiment, these biological samples may be sent to the fourth repository only upon the users' express instruction. Without such instruction, the biological samples will be destroyed immediately after the ordered tests are performed. If a user does request his or her biological sample to be kept and deposited to the fourth repository, he or she can take one or more additional steps with the biological sample, for example, order an additional test or rerun the ordered test as desired. Similar to the records in the second repository, or the databank, deposits in the fourth repository can be anonymous, for example, identifiable only by the unique password of the submitting user. A predetermined level of security (typically high) also can be implemented for the fourth repository. Therefore, a predetermined level
of security could safeguard a user's privacy if he or she elects to keep their test samples for future use or reference.

Therefore, different levels of security and privacy are provided for various information and sample repositories according to embodiments disclosed herein to serve different functions and purposes. Moreover, as discussed below, the level of privacy the users enjoy with respect to their test results and biological samples not only relies on the levels of anonymity and/or security of the repositories, but also can turn on one or more other characteristics of the systems and methods disclosed herein. That is, certain repositories can be insulated from other repositories, as desired. For example, in the embodiment above, the first and the second repositories can be substantially insulated from each other and, similarly, the first and the fourth repository can be substantially insulated from each other. Thus, repositories where higher levels of privacy and/or security are desired can be insulated from those that may operate with less stringent requirements of privacy and security.

The term “insulation” or “insulate” as used herein, refers to the substantially separate and independent existence and operation of the selected repositories, whether physically, electronically, or network-wise. Advantageously, there is complete detachment, whether physically, electronically, or network-wise. For example, a user may have entries in all the repositories, but he or she is only identified in the second and fourth repositories – the repositories endowed with higher levels of privacy – by a unique password created (or assigned) and controlled by him or herself. The unique password works with a unique identification code that may, for example, either be created by the user and communicated to the operator of the system or created by the operator of the system and communicated to the user anonymously. As such, the true identity of the user can be concealed from the operator of the system and yet the system is able to safely deliver the test result to the databank under the unique identification code which the user is able to track down and match with his or her unique password to thereby retrieve the results. Such retrieval can only be done by the user or a designee thereof who possesses both the unique identification code and the unique password.
Computer System for the Implementation of the Method

An example of an embodiment for the administration of the test is shown in Fig. 1. The computer system comprises a personal computer 10 at which the user of the test can order the test and through which the user of the test can retrieve the results of the test. The personal computer 10 includes a display device and runs a browser 15, such as Netscape Navigator or Microsoft Internet Explorer, which accesses a remote computer 25 through a network 20. The network 20 can be a local area network or a virtual private network (VPN), but is more preferably the Internet.

The remote computer 25 is running a network interface program 30 such as the Microsoft Internet Interface Server or an Apache Server. The interface program 30 accepts instructions from the network 20 and passes them through to a test administration program 40 that is running on the remote computer 25.

In one embodiment of the invention, the interface program 30 uses the HTTPS protocol according to SSL level 2 or 3 to transfer the instructions from the personal computer 10 to the remote computer 25. Alternatively, VPN-on-demand technology can be used to set up an encrypted channel over the network 20 between the personal computer 10 and the remote computer 25.

The test administration program 40 includes a database server 45 connected to a databank 50, which holds the results of the tests, a product database 52, which holds details of the tests that may be ordered, and an e-mail administration module 47 that is adapted to send e-mails over a further network 60. The database server 45 can be a database program such as MySQL, Microsoft Access, the ORACLE database system obtainable from Oracle, the Objectivity/DB system obtainable from Objectivity, Inc., or IBM DB2. The database server 45 is connected to a databank 50. The databank 50 can be stored in dynamic or static memory and, for faster access, may include caching systems as is known to the skilled person.

The test administration program 40 also includes an encryption program that is used to encrypt any medical and personal data sent from the personal computer 10 to
the remote computer 25 and for encrypting e-mails in the e-mail administration module 47. An example of an encrypted e-mail is shown in Fig. 3.

The test administration program 40 can further include a data analyser that can extract medical and personal data from the databank 50 and analyse the medical and personal data to obtain conclusions as explained below.

The database server 45 may also be connected to an annotation storage 57 which function will be explained later. The remote computer 25 may further include a knowledge base 55 or be linked through the network 20 to a knowledge base 55. The function of the knowledge base 55 will be explained later.

The remote computer 25 further includes a payment administration module 42, which is connected to a financial institution, such as the EasyCash Company in Germany. The payment administration module 42 takes details of the method of payment desired by the user of the test and passes it through a network 43 to the financial institution 44 for debiting from the user's bank or credit card account.

As will be explained in more detail later, the e-mail administration module 47 sends any data (including identity data) related to a user's order through the further network 60 to an intermediate storage area 70. In one embodiment of the invention, three intermediate storage areas 70 are used to ensure that no data is lost in the event of a breakdown of one of the intermediate storage areas.

A local server 90 is provided in a secure facility on which the details of the user's order are stored in a local storage 100. The local storage 100 only includes names and addresses of the users and will not hold test results. The local server 90 is connected to the intermediate storage area 70 through a network 80. The network 80 can be the Internet. In the preferred embodiment of the invention, the local server 90 is not permanently connected to the intermediate storage 70 but is only connected on-demand for short periods of time to download the data on the intermediate storage 70. After downloading of the data from the intermediate storage 70, the local server 90 is disconnected from the network 80 and the data deleted from the intermediate storage 70. The local server 90 can run any suitable operating system, e.g. Microsoft Windows or Linux, and network connection program. The local server 90 is
furthermore provided with an e-mail module and encryption software to enable it to read the e-mails downloaded from the intermediate storage 70. Decryption of the e-mails is only carried out when the local server 90 is off-line in order to ensure that access to the decrypted information is restricted. The local server 90 is furthermore provided with the necessary software to ensure that the user’s order is processed.

A testing center 110, comprising a laboratory and a computer system, is shown in the figures. The testing center 110 performs the tests in an anonymous manner and returns the results of the tests over a network 120 to the databank 50.

In addition to the Internet access through the network 20, the system also offers telephone access to the system. Registration may also be done by sending a postcard or letter to the administer/operator of the system. Pre-made registration postcards may be distributed by the operator/administrator of the system to facilitate user registration, which include check boxes for various tests offered, the methods of payment, and for requesting additional information on certain tests and services provided. The credit card information may also be transferred over telephone. Upon registration, a telephone number is provided to the user for future access of his or her test results, using, like the Internet access, the unique identification code.

**Ordering & Administration of the Test**

The privacy, anonymity, and security properties of some of the embodiments discussed herein can be further appreciated, for example, by examining the depiction of Fig. 2. Fig. 2 provides an overview of certain embodiments for ordering and anonymously administering one or more tests and for enabling personalized health risk assessment. Specifically, the following steps or processes may be performed.

In the first step 200, one or more users access a portal on the remote computer 25 at which information about the test can be viewed and the test can be ordered. Access to the portal is obtained by entering an IP address or a domain name in the browser 15 on the personal computer 10. The browser 15 accesses through the network 20 the remote computer 25 on which the test administration program 40 is
running. The user at the personal computer 10 can access details of the tests that can be ordered through database server 45. The database server 45 requests details of the tests stored in the product database 52 and returns these details in a displayable form to the browser 15.

In step 210, the user registers for the test. The registration is carried out by the user filling out a form displayed on his browser 15. This form includes the name and address of the user and the method of payment that the user chooses. The form may further include an acknowledgement of the general terms and conditions of the provider of the test and a liability exclusion. These details, together with the order number or name of the test, are encrypted using the encryption technology provided in the browser 15 and on the remote computer 30 and transferred through the network 20 to the remote computer 30.

At the remote computer 30, payment for the test is initiated in step 200. Processing of the payment is carried out in the payment administration module 42 as explained above. In step 225, details of the order are forwarded to the test provider. This is done by the test administration software 40 that co-operates with the E-mail administration module 47 to generate an encrypted e-mail 65 (such as shown in Fig. 3), which is passed through the network 60 to the intermediate storage 70. Details of the user and the test, which has been ordered, are not permanently maintained on the remote computer 30. Instead of an encrypted e-mail, encrypted data sets may be transferred.

In step 230, the test kit is sent to the user. The local computer 90 downloads at periodic intervals from the intermediate storage 70 the encrypted e-mails 65 and unencrypts them. The local computer 90 then generates a delivery note for the test kit dispatchers. The local computer 90 also generates a unique identity number for each user. The unique identity number is a ten-digit number and is sent with the test kit to the user.

The test kit dispatcher forwards to the user a kit or package that contains materials for taking a sample for the ordered test and instructions on how to collect the sample. The materials may include, among other things, sample tubes, antiseptic agents, and syringes. In one of the alternative embodiments, the kit further contains a
unique identification code, which has been created by the system, i.e., the operator or administer of the system, randomly and anonymously. Along with the kit, the unique identification code is sent to the user anonymously, that is, without any reference to the user's identity. In other alternative embodiments, the unique identification code may be created directly by the user and therefore remain known only to the user.

In step 240, the user receives the kit together with his or her unique identification code. The user takes a biological sample and returns the biological sample in step 250 to the testing center 110, which then analyses the sample and in step 260 provides the results of the test together through the network 120 with the unique identification code to the databank 50 on the remote computer 25.

Biological samples may be any sample containing genetic material, including for example, blood or blood components, palatal swaps (i.e., epithelial cells extracted from the mouth cavity), urine, and other human non-blood genetic material, among other things. In the alternative embodiment where the user creates the unique identification code, this code is transferred to the system or operator/administer of the system along with the biological sample, such that the test results may be recorded later under the corresponding code. It is to be noted that the biological samples and test results are only identified with the unique identification code known to the user; the system or operator/administer of the system has no access to the code and no way of linking the test results to the true identity of a registered user. The insulation between the databank 50 and the first repository on the local computer 90 enable such anonymity and privacy guard as discussed supra.

The test results may be accessed and reviewed only by the user, through a secured interface linked to the second repository. The user can access the results of the test in step 270 by means of the browser 15 and the database server 45 on the remote computer. The user enters his or her unique identification number in the browser 15, which acts as a validator by encrypting the number and passing it to the test administration program 40. The test administration program 40 decodes the unique identification number and passes it to the database server 45 which accesses the test results in the result memory 55 and returns it to the test administration
program 40. The test administration program 40 then passes the results to the browser 15 for display to the user in step 280.

The forgoing steps 210 to 290 allow substantially anonymous administration of one or more tests ordered by a user. To enable a user to make health risk assessment based on these test results, certain additional steps can be performed as discussed below.

*User-Enabled Health Risk Assessment*

In other embodiments, one or more systems and methods for enabling a user to assess heath risks are added to the above-described systems and methods. Skilled artisans will recognize many possible systems and methods for enabling a user to assess health risks on the basis of the test results obtained. A few examples are described below, but many others are readily possible.

One embodiment employs a classification schema based on the tests ordered by the user, which comprises a plurality of risk classes ranked from the lowest risk to the highest risk, relating to the one or more disorders of interest. The user may make personal health risk assessment with respect to one or more disorders by determining a risk class based on his or her test results.

For example, for a test that examines the sequences of one or more genes contributing to a disorder, a classification schema may comprise the following risk classes:

(i) risk class I, no increased genetic risk of developing the disorder. This class represents the homozygous wild type group; both alleles of the gene are normal. Usually this is the best class to be in.

(ii) risk class II, usually moderately increased relative genetic risk of developing the disorder. This class represents the heterozygous wild type – mutant group; one allele of the gene is mutated.
(iii) risk class III, usually moderately to severely increased relative genetic risk of developing the disorder. This class represents the homozygous mutant group; both alleles of the gene are mutated.

(iv) risk class IV, usually highly increased relative genetic risk of developing the disorder. The class represents the combination of several mutations in different genes contributing to the disorder; different alleles of more than one gene are mutated. This typically is the worst class to be in.

A risk class can be further divided into subclasses to take into account, for example, the environmental or behavior factors, such as smoking, anti-contraceptives, overweight, and immobilization. Skilled artisans readily will recognize various other possible classification schemes that are possible for use in such embodiments.

Consistent with the classification schema, the test results may be annotated by the system and stored in the annotation storage 57 to assist in the user’s understanding and interpretation of the results. Based on these results and annotation – if any – presented by the system, through the interface linked to the databank 50, the user will be able to determine a risk class for him or herself with respect to the disorder of interest. As such, a layperson with no special medical knowledge, according to this disclosure, will be able to self-classify his or her relative health risks and to follow suggested avoidance strategies without consulting a medical professional. Further professional consultation may be sought, however, as discussed above, if the user so desires. Typical situations for pursuance of further diagnostic or therapeutic assistance are those where a high-risk class has been identified. Therefore, by enabling self-assessment of health risks, the present disclosure empowers a user or a patient to act proactively in monitoring his or her health conditions and take preventative measures in managing potential health problems.

**Anonymous and Secured Repository For Genetic Samples**

In other embodiments, a fourth repository is employed in the methods and systems discussed above. This repository may be considered as a secured sample repository where biological samples such as genetic materials of a user are kept
substantially or completely anonymously, e.g., marked with a unique identification code or a unique barcode known only to the user.

The deposition of sample materials, such as biological samples discussed above or blood samples, in the fourth repository may only be authorized and effectuated by the user. For example, absent the user's express request, which may be transferred to the system through an interface such as the interface of the second repository (i.e., the databank 55), the sample materials can be destroyed after the ordered tests are performed. If a user elects to keep the sample materials (including biological molecules such as DNAs, RNAs, and proteins extracted therefrom), the sample materials (or the extracted DNAs, RNAs, and proteins) can be forwarded, following the completion of the ordered tests, to the fourth depository and stored, advantageously in a highly secured manner, under one or more identification codes unique to the user. This allows the user to order additional tests if new relevant genetic or other diagnostic tests become available, for example, on a later date, without having to collect the sample materials again.

Likened to the second repository or the databank 55, the fourth repository can include a high level of security and/or anonymity. In such cases, for example, only the user or patient has the unique identification code and the corresponding unique password required to access the confidential medical and personal data and sample materials. No third parties, including healthcare management and insurance companies, employers, and the system or the operator/administer of the system would be able to access these secured repositories. The users thus obtain a high level of anonymity and privacy when taking advantage of the secured electronic (i.e., the second repository) and physical (i.e., the fourth repository) databanks.

The fourth repository or the physical databank may be desirable to some individuals because a diverse array of technologies, such as nucleotide microarrays and protein chips, are becoming available in diagnostic testing, such that multiplexed and parallel testing are made possible. This will in turn facilitate, for example, better prediction of the contribution of multiple genes to the development and progression of certain diseases, since the relative genetic risks may be measured on a broader basis.
A Health Information System Further Linked Thereto

In another embodiment, the third repository or knowledge base 55 is employed in the methods and systems of this disclosure as discussed above. Advantageously, the knowledge base 55 is relatively comprehensive, and can include, for example, both genetic and non-genetic information of a user, in addition to general biomedical background information on human physiology, diseases, diagnosis and therapies. As such, the third repository may serve as a management system for users’ medical records or medical files. In some embodiments, the third repository can mirror the record holders or users as virtual patients and enables the self-monitoring and management of their own health conditions.

The third repository thus may be updated regularly to input information on newly available drug treatments, medical expert references, lifestyle recommendations, useful diets, additional relevant testing, and potential participation in clinical trials, among other things. The information update may be performed manually by professional curators or automatically by a computerized process, for example through the network 20.

Further embodiments contemplate the use of professional curators who possess expert medical knowledge; and who scrutinize and filter the information and selectively incorporate into the knowledge base 55. A computerized process is typically implemented as a peripheral application program to the database server 45. It can link to other medical databases and knowledge bases worldwide through the network 20 that are publicly accessible or that are proprietary but for which arrangements have been made to gain access. Further, it can extract and parse new information, compile useful knowledge, and load into the third repository. Such application program may be implemented in any suitable programming language, such as JAVA\textsuperscript{TM}, C, C++, Perl, CGI, among others. Also, the knowledge base 55 may employ a relational database management system such as the Oracle database system under the trademark ORACLE or an object oriented database management system Objectivity/DB under the trademark OBJECTIVITY/DB produced by Objectivity, Inc., among others. The content of the third repository may be cast in a
user-friendly language and format, such that it is easily understandable to a layperson with no biomedical background.

**Analysis of Medical and Personal Data by an Information Seeker**

As discussed above, an information seeker can carry out analysis of the medical and personal data stored in the databank 55.

Generally, the information seeker wishes to carry out a study on the genetic data, other medical and/or personal data stored within the databank 55 in order to obtain certain conclusions. For example, the information seeker may wish to correlate side effects of taking a drug with genetic disposition. A data analyser can be incorporated within the test administration program 40 to allow such studies to be carried out. Alternately or additionally, a separate data analyser can access the medical and personal data through the database server 45 through, for example, a network.

In order to carry out the studies, the databank should include not only genetic information, but also details of drugs taken by the user. In order to allow quality studies to be carried out, the databank 55 should also include information about the lot number of the medical, pharmaceutical or other product taken or used by the user.

The information seeker can supply the test kit for taking biological samples to the user directly, rather than having the user order the kit as described above. In this case, the user will still create a unique identification number without reference to the information seeker in order to preserve confidentiality of the medical and personal data. The first repository will include the identity data.

The information seeker can also reward the user for taking part in the test. For example, cash cards could be issued to the user that are activated on receipt of a code word. The user is supplied with the cash card on receipt of the test. After providing the biological samples, or after answering a questionnaire, the user is provided with a code word to activate the cash card. Alternatively, the identity data in the first repository is used in order to send cash cards directly to the user.
The conclusions obtained from the study by the information seeker can be used to change dosages, formulations or methods of application of, for example, pharmaceuticals. It is also possible, that such large-scale studies lead to the discovery of further functions of genes and proteins unknown to date. The information seeker can use these further functions to prepare optimize or prepare new pharmaceuticals.

Specific embodiments of the disclosure are described by the following examples, which are illustrative but do not limit the disclosure herein in any manner.

**Example 1. Anonymous Administration of Human Diagnostic Tests**

The methods and systems of the present disclosure are particularly useful for anonymous administration of diagnostic tests that typically require high level of personal security and privacy, e.g., genetic tests, tests for sexually transmitted diseases, paternity tests, and tests for drugs of abuse. According to the embodiments disclosed herein, only the user, or any person or entity he or she entrusts, will have access to the test results. Neither the testing center 110 – which technically performs the test – nor a physician, an Internet provider, a telephone operator, the operator/administer of the system or the system itself would ever know the user's test results. The complete insulation between the first and second repositories and the complete insulation between the first and the fourth repositories, as discussed above, ensure the requisite anonymity and privacy.

Upon registering with the system, the user may order (step 210) the required test through the Internet (e-mail), telephone, fax, letter, postcard, preprinted order card, or in person. The user may be charged a fee (step 220) before he receives a service package or a kit. The payment may be by a credit card, money order, check, cash, cash on delivery, or through any other electronic paying system.

After receiving the money for the ordered test(s), the system or the operator/administer of the system will forward to the user (step 230), by any delivery
or parcel service or registered mail, an individualized service package or kit, which comprises the following items:

(i) a packing list;

(ii) materials for taking the sample, including sample tube, buckle swaps, or a syringe(s), used for collecting sample specimen, and any other tools, fluids, or accessory materials such as antiseptic agents that are necessary for the ordered test;

(iii) instructions for taking the sample, including explanations on how to use the materials and agents provided, how to collect the sample, and how to get professional help for taking the sample;

(iv) information about the ordered test(s) and the range of possible results and their risk implications and possible consequences;

(v) a voucher for the ordered test(s);

(vi) a unique secure and confidential data mailer envelope with four layers of packaging materials, three layers being sealed together as an envelope which contains a printed unique identification code and a barcode adhesive encoded with the same anonymous and unique identification code;

(vii) a sealed data sheet containing the Internet address which linked to the system or the operator/administer of the system – particularly, e.g., the interface of the databank – and a unique identification code assigned, anonymously, to the user, which allows the user to access the test results that will subsequently be stored in the databank 50;

(viii) a self addressed, pre-stamped, prepaid envelope or small parcel to mail the sample and voucher back to the system or the administer/operator of the system without any personal user identity data; and

(ix) a special adhesive sealing tape to ensure that the envelope cannot be opened without breaking the sealing tape.
The aforementioned unique data mailer envelope may include further specifics as follows: Page 1 contains a unsealed cover sheet which may be taken by a third party mailer or processing entity before shipping to the system or the operator/administer of the system. Page 2 is the face of the sealed unique data mailer envelope; it is of nontransparent packaging material. Page 3 contains a printed unique identification code and a barcode adhesive encoded with the same anonymous and unique identification code; it is of nontransparent packaging material. Page 4 is the backside of the copies of the unique identification code and barcode; it is of nontransparent packaging material. Pages 2, 3, and 4 are sealed together and made easy for the user to check for any broken seal.

After receiving the service package (step 240), the user compares the packing list with the delivery and examines whether the voucher corresponds to his or her order and whether the secure and confidential data mailer envelope is damaged or the sealing is broken. If there is any damage or the sealing is broken, the user may return the package and contact the system or the operator/administer of the system for delivery of a substitute package.

If the package is intact, the user may open the sealing of the data mailer envelop in a secure and private surrounding – typically his or her home (usually his living place). After taking sample specimen, the user may peel off the adhesive barcode label and attach the label on the sample container such as a sample tube containing his or her sample specimen. The user may then put the labeled sample and the voucher into the pre-stamped envelope and seal it with the special adhesive sealing tape and ship it to the designated address (step 250).

Upon receiving the sample, the system or operator/administer of the system may mark a note of arrival in the databank under the user’s unique identification code and specify an expected date when the test result may be available. In the case where a sample envelop with a broken seal is received, the operator/administer of the system will mark a note of broken seal instead, under the user’s unique identification code. The user can thus be notified and may request a new service package or kit from the system.
The system or the operator/administrator of the system may send the bar-coded, anonymous sample to an approved and certified contract laboratory. The test results may be returned from the contract laboratory marked consistently with the user’s unique identification code. Thereafter, the test results may be transferred to the databank 50, anonymously (step 260). Only the user is able to access (step 270) the server system, i.e., the interface of the databank, using his unique identification number and a unique password he had created previously that corresponds with the unique identification number.

The test results may be available on the data server, i.e., through the interface of the databank, for a defined time that, for example, corresponds to the user’s registration and the fee paid. The user has the option to view or print his test results (step 280); and, additionally, the user may elect to transfer the results to the system’s third repository system, the long-term and comprehensive medical knowledge base 55, as discussed supra.

Example 2. Genetic Risk Factors In Hemostasis And Deep Vein Thrombosis

Certain individuals are genetically predisposed to develop deep venous thrombosis (DVT), which may lead to fatal lung embolism, especially when subject to immobilization during long-haul air travel. The mortality rate caused by DVT is evidently higher than the mortality rate from aircraft crash. Recent studies indicate that there may be an increased frequency of DVT in the lower limb during long-haul air travel; symptom-less DVT might occur in up to 10 % of long-haul air travelers (The Lancet, 357, 1485-1489 (2001)).

The two most common genetic risk factors in patients with DVT is a single G-to-A base change at nucleotide 1691 (G1691A) in the factor V gene, termed factor V Leiden (FV-Leiden) – and a single G-to-A base change at nucleotide position 20210 (G20210A) within the 3’-untranslated region of the prothrombin (PT) gene. The FV-Leiden mutation appears in 20-60 % of patients with a known DVT history examined for a predisposition to DVT and occurs in approximately 5 % of the western population.
Mutation screening therefore can classify long-haul airline travelers into two categories: those who are required to take precautions to prevent development of DVT (e.g., taking oral anticoagulants or wearing anti-thrombotic stockings) and those who are not subject to increased risks of DVT. Access to this genetic test is thus of great importance to the potential predisposed individuals. Airlines, for example, also have a strong interest in encouraging their passengers to take such test and become aware of their possible predisposition to DVT.

The test of FV Leiden / PT gene for DVT may be administered in an anonymous and secured way for the travelers according to the present embodiment. A traveler or user may choose to order the test by registering through the Internet, by mail, or by telephone phone, as discussed supra. Billing will take place upon registration. A kit then may be sent to the user that comprises a palatal swap device, a unique identification number, and the information about taking the test and explanation of different results.

The user retrieves the palatal swap, puts the buckle swap device back in the enclosed transport tube and ships the whole package, together with the items described in Example 1, back to the system or the operator/administer of the system. The test results will be available for the user to access via the interface of the databank as described supra, e.g., over the Internet or a telephone. The user may determine his or her risk class based on the test results, according to the classification schema as follows.

FV-Leiden:

Class I: no mutation in both alleles ("homozygous wild type", no increased genetic risk to experience DVT episodes);

Class II: mutation(s) in one of the alleles ("heterozygous wild type / mutant", moderately increased genetic risk to experience DVT episodes, three to eight fold greater risk for thrombosis compared to class I individuals);
Class III: mutation(s) in both alleles ("homozygous mutant"), strongly increased genetic risk to experience DVT episode, 100-fold greater risk for thrombosis compared to class I individuals); and

**FV-Leiden / Prothrombin:**

Class IV: mutations (heterozygous / homozygous) in both genes: very strongly increased genetic risk to experience DVT episodes, 100-fold greater risk for thrombosis compared to class I individuals).

Additional subclasses may be included to account for non-genetic factors, such as environmental and other factors. That is, for example, individuals that belong to classes II, III, and IV may increase their risk levels if they are subject to smoking, oral contraceptives, older age, immobilization, or other coagulation system defects. Also, risk levels may be adjusted for users who had suffered multiple thrombotic events, who have family histories of thrombotic events, who suffered the first thrombotic event at young ages (under 40 to 45), who suffered thrombosis at an unusual anatomic site, e.g. outside the veins of the legs, pelvis, lungs, arms, cerebral veins, or eyes. The users of classes II, III, and IV may be advised to take additional genetic tests on the gene encoding methylenetetrahydrofolate-reductase (MTHFR), since it is known that a mutation in this gene (MTHFR-A223V mutation) contributes to a multifold additional risk increase to experience thrombotic events.

Other examples on genetic testing include coagulation and thrombotic disorders, hemochromatosis, breast cancer (e.g., BRCA1, BRCA2, others), colon cancer, others cancers, predisposition in drug response genes (e.g., genes for drug metabolizing enzymes like CYP450, and many others), drug receptors (Ah-receptor, vitamin D receptor, LDL receptor), transporters (e.g., serotonin and dopamine transporters) and many others.

Additionally, tests for drugs of abuse, HIV, tests for paternity and other forensic testing may be similarly administered.

It is understood that the above systems are applicable to humans as well as animals, plants, and any other organism for which such testing is desired.
Example 3: Questioning Consumers

The method and system for the analysis and correlation of medical and personal data of the invention can also be used to strengthen the relationship between the test subject as a patient and a manufacturer of pharmaceuticals. The test subject can be sent a questionnaire using the identity data stored in the first repository. The questionnaire will include a unique identification number under which the results of the questionnaire are stored in the second repository 50. The selection of test subjects to whom the questionnaire is sent can be obtained, for example, through a known list of customers or by a request for volunteers placed in various media. The test subjects could then register their interest over the Internet or by telephone.

The questionnaire could include information relating to the age, known diseases, lifestyle, dietary habits and pharmaceuticals currently being taken or having been taken in the past. The questionnaire might also be part of a test kit including, for example, swabs or other means to take samples from the test subject.

As an incentive for participation in the study, the test subject can be supplied with a reward such as a cash card, telephone card or other voucher or incentive, which will be activated after receipt of the questionnaire. This could be done, for example, by providing a personal identification number or other authorization code to the test subject on receipt of the questionnaire.

One example of a questionnaire that might be distributed is a study on the effects of “lifestyle” drugs such as drugs to overcome erectile dysfunction problems in men. The questionnaire might include questions relating to the sexual behaviour of the test subject before and after taking the drug. Only the results of the questionnaire are stored in the second repository – the identity of the test subjects is unknown.

It is envisaged that correlating the results of such studies the efficacy of many pharmaceuticals can be improved by correlating their effects with different personal and medical data. It is further anticipated that new effects and possible indications of drugs can be identified by statistical analysis of the medical and personal data acquired.
Example 4: Strengthening Relationship between Customer and Manufacturer

The invention can also be used to strengthen the relationship between a customer and a manufacturer. For example, a customer who had purchased a certain number of products could forward to the manufacturer proofs of purchase, such as a receipt or a portion of the packaging showing the lot number. The customer could also return to the manufacturer a questionnaire or biological sample together with the proofs of purchaser.

After return of the proofs of purchase, the customer could be rewarded as described in Example 3. Return of the proofs of purchase could also enable the customer to be authorized to re-purchase the product. Taking the example of the lifestyle drugs mentioned above, the customer could be supplied with a new prescription on return of the proofs of purchase. Alternatively, the instructions to provide the customer with a further supply of the product could be communicated to a pharmacist.

It is further to be understood that the description, specific examples and data, while indicating exemplary embodiments, are given by way of illustration and are not intended to limit the invention(s) described by the appended claims. Various changes and modifications within the invention(s) defined by the appended claims will become apparent to the skilled artisan from the discussion, disclosure and data contained herein, and thus are considered part of the invention(s) described by the appended claims. In the appended claims, the articles such as “a,” “an,” “the” and the like can mean one or more than one, and are not intended in any way to limit the terms that follow to their singular form, unless expressly noted otherwise. Unless otherwise indicated, any claim which contains the word “or” to indicate alternatives shall be satisfied if one, more than one, or all of the alternatives denoted by the word “or” are present in an embodiment which otherwise meets the limitations of such claim.
CLAIMS

1. Method for the analysis of anonymous data comprising the following steps:
   - obtaining from the test subject at least one item of anonymous data,
   - anonymously recording in a second repository (50) the at least one item of
     anonymous data under a unique identification code,
   - extracting from the second repository (50) one or more of the at least one item of
     anonymous data, and
   - reporting a conclusion from the anonymous data.

2. Method according to claim 1, wherein the at least one item of anonymous data is
   obtained from a test laboratory to which the test subject has provided a sample.

3. Method according to claim 2, wherein the sample is obtained from a test kit ordered of
   anonymously by an orderer.

4. Method according to claim 2, wherein the sample is obtained from a test kit supplied
   by an information seeker.

5. Method according to any of the above claims wherein the at least one item of
   anonymous data is a lot number of a medical or pharmaceutical product.

6. Method according to claim 4 or 5, wherein the information seeker is a pharmaceutical
   company interested in the effects of pharmaceuticals on the test subject.

7. Method according to claim 6, wherein the at least one item of anonymous data
   includes an indication of side effects of the pharmaceuticals.

8. Method according to any of the above claims wherein the at least one item of
   anonymous data includes genetic data.

9. Method according to any of the above claims wherein the step of reporting of the
    conclusion includes gene epidemiology data.
10. Method according to any of the above claims wherein the at least one item of anonymous data includes a pointer to a sample store.

11. Method according to any of the above claims, further comprising a step of storing identity data relating to the test subject in a first repository insulated from the second repository.

12. Method according to claim 11, further comprising the use of the identity data to question the test subjects.

13. Method according to claim 11 or 12, further comprising the use of the identity data to reward the test subjects for supplying the at least one item of anonymous data.

14. Method according to any of the above claims, wherein more than one conclusion is reported.

15. Method according to claim 14, further comprising the step of correlating the more than one conclusion in order to obtain statistically relevant data.

16. Method according to claim 1, wherein the unique identification code is initially concealed.

17. System for analysis of anonymous data comprising:
   - a first repository (90) for the storage of identity data;
   - a second repository for the storage of at least one item of anonymous data, the second repository (50) being isolated from the first repository (90);
   - a data analyser connected to the second repository (50) and isolated from the first repository (90).

18. The system of claim 17, wherein the anonymous data is data relating to the genetic composition of the test subject.
19. The system of claim 17 or 18 further comprising a third repository for the storage of a sample referenced by the at least one item of anonymous data.

20. The system of any one of claims 17 to 19, further comprising a reward card.

21. A method for anonymously administering at least one test for one or more test subjects, comprising:
   a) registering (210) one or more orderers by recording, in a first repository (90), the identity data thereof;
   b) forwarding (230) to each of said orderers, without referencing the identity data of the one or more test subjects, a kit which comprises (i) instructions on and (ii) materials for taking at least one sample for said at least one test;
   c) receiving (240) said sample from the test subject;
   d) obtaining, for each test subject, a result of said test on said at least one sample; and
   e) recording (270), in a second repository (50), said result for each of said test subjects under a unique identification code, wherein the first repository (90) and the second repository (50) are insulated from each other.

22. The method of claim 21, wherein said unique identification code is created by each of said orderers and wherein the receiving further comprises receiving said unique identification code.

23. The method of claim 21 or 22, wherein the test is a diagnostic test for a disorder selected from the group consisting of coagulation and thrombotic disorders, hemochromatosis, cancer, and HIV, or the test is a genetic test for one or more genotypical or phenotypical traits.

24. The method of any one of claims 21 to 23, wherein each of said test subjects further creates a unique password which corresponds to the unique identification code, said method further comprising allowing each of said test subjects to access said result under the unique identification code in the second repository (50) using said unique password.
25. A system for anonymously administering at least one test for one or more test subjects, comprising:
   a) a first repository (90) having stored therein the identity data of said one or more orderers, entered by said one of more orderers upon registration;
   b) a kit comprising instructions on and materials for taking a sample for said test, forwarded to each of said test subjects with a unique identification code;
   c) a unique password created by each of said orderers, which corresponds to the unique identification code; and
   d) a second repository (55) having stored therein, under the unique identification code for each of said test subjects, a result of said test on said sample, said result being accessible to the test subject on receipt of the unique password.
   wherein the first repository (90) and the second repository (55) are insulated from each other.

26. The system of claim 25, further comprising a first interface (30, 40, 47, 70) capable of receiving the identity data entered by each of said orderers upon registration, wherein said first interface (30, 40, 47, 70) connects to said first repository (90).

27. The system of claim 26, wherein the first interface (30, 40, 47, 70) comprises a first data transfer system (47) for transferring the identity data to an intermediate storage (70) and a second data transfer system (90) for transferring the identity data from the intermediate storage (70) to a local storage (90).

28. The system of one of claims 25 to 27, further comprising a second interface (40) having a password storage area and capable of providing the result of said test under the unique identification code when the unique password is entered by each of said test subjects, wherein said second interface (40) connects to said second repository (55).

29. The system of one of claims 25 to 28, further comprising a third repository (55) connectable to the second repository for studying the health conditions of the test subject and/or assessing the health risks of the test subject.
30. The system of one of claims 25 to 29, further comprising a fourth repository capable of storing, upon an instruction from each of the test subjects, said sample or biological molecules derived therefrom.

31. The system of claim 29, further comprising a classification schema stored in the third repository (55) and based on said test, wherein the classification schema comprises a plurality of risk classes ranked from lowest risk to highest risk, relating to said one or more disorders.

32. The system of claim 31, wherein said kit further comprises information on said classification schema, allowing the test subject to self-assess the personal health risks relating to said one or more disorders by determining a risk class based on said result of the test.

33. A computer-readable medium (50) having stored therein a data structure, comprising: one or more first fields containing anonymous data representing results of one or more tests performed in accordance with the method of one of claims 1 to 4; and a second field containing a unique identification code permitting access by the test subject to said anonymous data in said one or more first fields.

34. The computer-readable medium of claim 33, wherein said data structure further comprises a third field containing a unique password created and supplied by the test subject, said unique password corresponds to said unique identification code thereby permitting access to said data in the one or more first fields.

35. A computer-readable program (15) in a computer system (10) having a user interface, said computer-readable program having computer instructions for accessing results for one or more tests stored in a databank (50), said one or more tests being performed in accordance with the method of one of claims 1 to 16 or 21 to 24; validator (15) for providing to the databank (50) an unique identification code, said unique identification code permitting access by the test subject to said results in the databank (50); and display device (10) for displaying on said user interface said results.
36. A test kit for anonymously administering a test in accordance with the method of one of claims 1 to 16 or 21 to 24, comprising:
   instructions for administering said test;
   materials for taking said sample for said test;
   a unique identification code capable of identifying said sample and permitting access by a test subject to results of said test.

37. The test kit of claims 36 in which the unique identification code is initially concealed.
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: For info see http://www.gnupg.org

hQEOA1bMJaxKA/jjEAP/WWN9mYReJITYYQ16jdbhmWI2Yi1CXWnuGlyy0G3Jr1Kg
omrMjIGKLay/0PhrGn9EaTn+7TnUNTOIVV0caJueTzw6X+gH9HWqpmwugYuoXIwA
a/568FPzS6Kb/isU4OhVXTRdQGeicPCNajwNohXWxOn2g2xhd6FAdxTrzJY052UO
/D6Xxa6itIsQQUzdHidqPJwF16Sgw7yjJaNz99q3MG1CZDDf1Vx4y5pUfm/ln8qP
uQ0mlIs7dck+a2bJ/Oh0p+gC/MMLY/O/7qFagroRADI1Kqy0M4+gQDRyz51vtga1V
NbzSFDmsS85cN4E87yJg9aXN9UaIdfPUJJLw7jH1WzdAx0se/AeOKmhi8MLGj9riZJ
N3e8BTArifoJY3h6R2D7U72h2Vxzf2K7224fCmZ6J63+11aGi5jWae16mzK2Q9kP0Nq
UVsRLOQ9JO4gddO9xeXTUCLcVhYj1kKF91NMX7gwx+wH5C48a51JzLYeiaOBVr9F
yNJJziu9ENQX8nayNDFKvDwpo5FQ2yNyRBmhxlxtj+krgd4ixVyk2YRTejj0UXh
JPEhm/gMEslYXeYCr8rn0SjNzgyKRYHkFwq34IrPut0aUYJjo7wSIq5XWeMvOx
zAvXO83/Izjn0t6DKVmuVtxpub5wyUH1kpxF1ryWMyrGcEz4UscZBFyj+7EsV6S
GY4BT6rdKfyFPkoUAgAVu7Vb5BhtVYns4Bkqg1eA/9S8pzirUKUHvdF3i0b+3Qg
YlkONYF21hnm8eb0cFIAGc60/+0Hkhk3ct7RFW0rbtk2jynqdkNh2RbNxxQ2j32dZ
JxmJedRoyV71YPA0BmEcrSzUEuaoYVFesIVjYkYdx+46bM9m0AU7v2WFNO/Dmck/
w7jD0UEF8eaAVP8aLYzmzS7D4YtFaJUaS1Wm7T3RVJ14+VCJ6pKm5KoeEUEx1
zY2ysd9s+0xpMqOBQwCIZeODRo+3UCiXQMa6r116a3UbMmRi0EWPMsFqgm4wuac1L
bjm0YrgU7wuuULcxUGhs/ubUQ==
=Dkk7
-----END PGP MESSAGE-----