|LAW AUDIENCE JOURNAL|
|VOLUME 1|ISSUE 4|JUNE 2019|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2018): 2.06|

|LAW AUDIENCE JOURNAL®|

|VOLUME 1 & ISSUE 4|

|JUNE 2019|

|ISSN (O): 2581-6705|

EDITED BY:

LAW AUDIENCE JOURNAL'S

EDITORIAL BOARD

|LAW AUDIENCE JOURNAL|
|VOLUME 1|ISSUE 4|JUNE 2019|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2018): 2.06|

Email: lawjournal@lawaudience.com, info@lawaudience.com,
Phone: +91-8351033361,
Website: www.lawaudience.com.
Facebook: www.facebook.com/lawaudience
Instagram: www.instagram.com/lawaudienceofficial
Contact Timings: 5:00 PM to 9:00 PM.

DISCLAIMER:

Law Audience Journal (ISSN (O): 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however, the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in Volume 1 & Issue 4 are the original work of the authors.

Views or Opinions or Suggestions, expressed or published in the Journal are the personal point of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work.

All disputes subject to the exclusive jurisdiction of Courts, Tribunals and Forums at Himachal Pradesh only.

|LAW AUDIENCE JOURNAL|
|VOLUME 1|ISSUE 4|JUNE 2019|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2018): 2.06|

"CHALLENGES BEFORE DATA PRIVACY LAWS IN INDIA: WITH SPECIAL REFERENCE TO PROTECTION OF PATIENTS INFORMATION."

Authored By: Mr. Ilayanambi.B (B.A.LL.B (Hons)),

Tamil Nadu National Law University.

Email Id: nambi161096@gmail.com.

Published At: https://www.lawaudience.com/volume-1-issue-4/

I. INTRODUCTION:

"It is pertinent to know the importance of the patient's data and the analysis of the treatment provided, but the patient treatments confidentiality is of utmost importance because it is directly attached to the fundamental rights of the patients Right to Life, Liberty and Privacy. So, providing patients information is subject to individual confidentiality and it differs from patient to patient. Hence protecting patient's information is necessities, which nowadays are stored more often in electronic records which has more chance to be exposed because of persistent threats like hacking etc. Anonymous information of a patient requires the data controller to make changes to the information provided by the data subjects and filter all the personal details.[1] *And moreover, the information should be in such manner that, the processor who has the information should not be able to identify the personal information of the de-identified subject. Accessing the personal information of the patients without authorization is a punishable offence*[2] *in the United States under Part-C of the Health*

[1]"L.Sweeney,*Patient Identifiability in Pharmaceutical Marketing Data* available at http:// dataprivacylab.org/projects/identifiability/pharma1.pdf. (Accessed on 29.03.2019)".

[2] "J. Kulynych & D. Korn, *Use and Disclosure of Health Information in Genetic Research: Weighing the Impact of the New Federal Medical Privacy Rule*, 28 Am. J. L. And med. 309 (2002). (Accessed on 29.03.2019)".

Insurance Portability and Accountability Act, 1996 (HIPPA).[3] *European Union Directive, 1995 has a similar principle to that of the US with regard to the Personal information of the patient, specified under EU data protection directive.*[4] *Although this process seems to be an alternative but the process of anonymization can be ineffective sometimes, where even the de-identified information can be traced back to the subject.*[5]

The electronic records of the individuals had been exposed at various stages & circumstances, which lead to the identification of risk at different stages. So, to avoid this there are two options for the data protectors either to anonymize the information that possesses the risk of identification or to make it available only to the Physician. "But, finding and introducing a mid-path is the only feasible solution to this Ethical dilemma that has been created because the above mentioned first option, which is rendering information anonymously is not feasible because there is a chance of misusing of information by the intermediaries but this option, if governed by set of rules and regulations, can be led the way for solution."

Then comes the second option which is also not feasible, because of the complication in the Physician-Patient relationship that exists between them because of the presence of other Stakeholders, Insurers and Pharmaceutical Manufacturers. But the Indian government has taken a step forward by introducing NeHA, the Ministry of Health in 2015, introduced NeHA (National eHealth Authority) in order to regulate the maintenance of electronic records in India and also to cope up India with that of the International standards, and acting on its

[3]"Health Insurance Portability and Accountability Act, 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) ('HIPAA 1996')."
[4]"Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJL 281 ('Data Protection Directive')."
[5]"Supra note-1, ("A study on the possibility of re-identification showed that patients with HIV are susceptible to being identified by employers who have access to sensitive health information. This concern was also raised by the European Court of Human Rights in I v. Finland, Application No. 20511/03: 2008 ECHR 623 (17 July 2008)")".

aim, NeHA has introduced DISHA a Draft Bill in 2017, which is still pending to be passed. However, to make it alongside the International Standard, the Indian Government had enacted the IT Rules "Reasonable Security practices and procedures and sensitive personal data or information", 2011.[6] *The rules 6, 7 & 8 of the IT Rules require Disclosure and Security requirements in handling Sensitive data protection.*

In this research paper, the researcher presents an overview of various data protection regimes of various countries such as EU, UK & US followed by the analysis of Indian Position. The researcher also analyses the DISHA, 2018 Bill, which is primarily a Health Care Data Privacy Act. The researcher discusses its use and contemporary Issues involved in it. Followed by it this paper also accesses whether the new rules make any difference in patient's privacy in India. Cause the new rule prohibits the unauthorized use of medical information.[7] *And more importantly after a major security breach in London, involving thousands of breaches of Patients records in National Health Service (NHS), even though the new effective law of India already exists there.*[8] *This possesses a serious threat to the existing nature, which requires more effective privacy-enhancing technologies."*

II. INDIVIDUAL DATA AND RIGHTS PROTECTION IN EU, US & UK:

Not all information seeks protection under the Data or Information Protection laws but that information which contains a certain amount of sensitive information in it does. Only certain information handled by data processors and data controllers[9] can be considered Personal and only such information's are triggered for protection under this regime. The information that

[6] "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011."
[7] "Rule 5(2) of IT Rules, 2011."
[8] "Press Association, *Tougher Penalties Planned for NHS Data Losses*, The guardian (London), July 1, 2011"
[9] "UK Data Protection Act, 1998 (c. 29), S-1(1) (This implementing legislation ensures compliance with the data protection principles enunciated in the Data Protection Directive)."

affects the Individual privacy is considered to be the Personal information[10], and the controller or the authorized person by such controller is responsible for such Data of the subjects processed and the manner of the data processed.[11]

II.I EU'S POSITION ON HEALTH INFORMATION AND MEDICAL HISTORY AND ITS PRIVACY:

EU member states data protection laws are more based on the EC Data Protection Directive. Fair and lawful processing of the personal information was the core principle of data protection regime[12] and such information must be obtained for lawful specified reasons and should be processed adhering the purpose.[13] And the data provided is also subject to the time limit and the person receiving the data should no longer possess the information once the specified purpose has been fulfilled or the time limit has been elapsed. And it is also the duty of both Processor and the controller to prevent any unlawful use of protected information and they also have an obligation to enforce appropriate organisational and technical measures to prevent or avoid any unlawful breach and processing.

The Directive also takes care of the cross-border health care and research and lays down a general presumption on the adequacy of the data protection laws in the Third Countries.[14] It also requires equivalent protection of personal data through minimum security requirements for the data shared by patients across the EU. When the transfer takes place between states that follows the Directive the Controller can treat the transaction as of the host country[15] but if not then the data protection law of the third country would be evaluated based on the

[10] "Durant v. Financial Services Authority, 2003 EWCA Civ 1746."
[11] "UK Data Protection Act, 1998, s.1(1)".
[12] "Data Protection Directive (These principles were part of the Council of Europe's attempts to harmonise national laws on data protection in its 1973 and 1974 resolutions, and are laid down in Schedule I of the Data Protection Act, 1998)".
[13] "UK Data Protection Act, 1998, Schedule 2 and 3."
[14] "European Protection Directive, Articles: 25 & 26."
[15]"Health Systems governance in Europe: The Role of EU Law and policy 564 (E. Mossialos, G. Permanand, R. Baeten & T. K. Hervey eds., 2010)."

Circumstances such as nature of data, its purpose and its duration. In 2008, in the case of ***I v. Finland***[16], the European Court of Human Rights elucidated the importance of health data protection and a person's right to privacy, in this case an employee of eye clinic and also a former patient of that clinic, whose HIV status has been revealed due to the easy access to the patients register that contains sensitive information like treatment and diagnosis information. The European Court of Human Rights, in this case, observed and held that sensitive information regarding patient's details must be kept away and safe from the unauthorized use.

The EU's new regulation on the personal data was published in May, 2016, in which patients right to be heard, Right to rectification, Right to Erasure, Right to transfer, Object and access one's own information has been enforced and ensured and the Rights and limitations of the patients data organisations were established and more importantly an exception clause of "Research work" has been introduced in order to develop the health sector but it is subject to the condition of patients right to be heard where it is mandatory to inform the patient of such use of information and the risk involved in it. The new regulation provides a clearer view on patients and citizen's rights than the previous one and the EU's perspective is to continue to collect and communicate patient's perspective on protecting and sharing of patient's data.[17]

II.II UK'S STAND UNDER UK DATA PROTECTION ACT, 1998:

Usually, there is no ethical dilemma between health care experts with regard to anonymous information. Personal data is defined under S.1 (1) of the DPA as "data which relate to a living individual who can be identified- (a) from the data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller." "The EC Data Protection Directive states that "the principles of protection shall

[16] "*See* I v. Finland, Application No. 20511/03: 2008 ECHR 623."
[17] "The new EU Regulation on the protection of personal data: what does it mean for patients? A guide for patients and patients' organisations, European Patients Forum (EPF), pg. 1-22."

not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."[18] The level of protection ordinarily afforded to the personal data cannot be decreased for the cause of de-personalisation of patient data and thus the anonymisation of data should not be the only factor dissident for the test for depersonalization of data.

The European Court of Human Rights emphasized the importance of the concept of "private life" in a recent judgment[19] and gave a wider interpretation to the concept by including a person's life, his family, and his health information, which can be conclusively said that it's a person's right to access and protect all aspects of his own. And this view had been outlined by the Court of the appeal of UK in the case of ***R v. Department of Health, Ex p Source informatics***,[20] in this case, a company which collects de-personalized data from pharmacists had an intention to sell it to ascertain the prescribing method of general physicians. "The Court of Appeal held that no duty of confidence arises in relation to fully anonymised information. This line of reasoning fallaciously assumes that a patient's reasonable expectation of privacy is limited to primary uses of identifiable information."

As per S. 11 of UK's DPA Act, 1998, an individual has the right to be heard and Right to prevent his data from Commercial exploitation through a notification to the data controller and unlike the Source Informatics case, commercially exploited anonymized information must be notified to the data subject, as to what's the purpose behind such notification.[21] Further, in S. 1(1) of DPA Act, 1998, it defines "Processing as "alteration or Adaptation" which ultimately includes that a patient whose data is being De-personalized must be notified the purpose of such De-personalization.[22] It is not appropriate to assume that the data controller is relieved from his obligation to comply with the Data Confidentiality once the

[18] "Data Protection Directive, Recital 26."
[19] "S and Marper v. UK, (2009) 48 EHRR 50."
[20] "(1995) 4 All ER 185, rev'd (2001) QB 424 (CA)".
[21] "*See* principles of medical Law, supra note 15, 659."
[22] "Supra note 9."

information has been anonymized because there are exceptional circumstances that would create liabilities.

In case of ***Common Services Agency v. Scottish Information Commissioner***,[23] information regarding the childhood leukemia was disclosed and such disclosure was refused by the Common service agency because there was no direct disclosure however the information was leaked due to its rare case of disease suffering individuals in the locality. In this case, the House of Lords held that the Anonymized information should be sufficiently De-Personalized before any disclosure and the case was remitted to the presence of Information Commissioner. Under UK's law, the use of patient's Identifiable information is strictly prohibited but both its law and the Judiciary is unclear about its stand in the cases where the patient's information is anonymized but still might pose a risk. And there are no clear-cut regulations or appropriate organisational and technical approach. Whereas this being the UK's Stand, the EU based its stand on Rights-Centric approach.

II.III UNITED STATES POSITION:

In the US the Electronic transmission of patient's information which is governed by HIPAA (Health Insurance Portability and Accountability Act, 1996, has been improved through the "Efficiency and Effectiveness" of the health care system by the establishment of Standards and requirements for such transmission.[24] And also the information collected and the individuals' privacy has been ensured at various stages. Patient's anonymity is ensured at various stages of data collection, data processing and Disclosure.[25] There are limitations laid down for such collection, some data are collected anonymously at the time collection of information itself which serves the purpose and further the range and purpose of the

[23] "(2008) UKHL 47."
[24] "HIPAA, 1996, S. 261."
[25] "N. P. Terry, *Symposium: The Politics of Health Law: Under-regulated Health Care Phenomena in a Flat World: Medical Tourism and Outsourcing*, 29 W. n Eng. L. Rev. 441 (2007)".

collection can be narrowed and limited to the purpose such as Treatment, research etc.[26] However, due to the rise of Commercialization the limitations and other systems tilts towards the failure and other Stakeholders like corporate entities slowly gains the stronger access of the patient's information[27] and the health information of the patients if identifiable leads to the commercial exploitation of information.

HIPAA fails in providing a strict application with regard to the process of patient's information and it also does not speak about the Consent to be given by the data subject. Since the growth of the market for the patient's data all around the World, other than the Food and drug administration in the US,[28] the entities like insurers, researchers and drug manufactures continuous uses the health information in commercial manner and there is no effective legislation to this extent which protects the patient's information from the exploitation and no state legislations could prevent the sale of patient's information and further could not defend their legislations against the data mining companies which claims that such laws affect their fundamental rights.[29]

Corporates had been given a free rein to abuse the patient's information legally[30], after the Vermont law which had laid restrictions on the nature of the information itself and the usage of information and also on the specified purpose, A Prescription Confidentiality law was struck down by US Supreme Court. In this case, since the state was unable to establish that the statute had "Substantive State Interest" and further the court found that "The content-based burden in S. 4631(d)[31] of the Vermont statute affected expression protected under the

[26] "id".
[27] "Jeroo S. Kotval, *Market-Driven Managed Care and The Confidentiality of Genetic Tests: The Institution as Double Agent*, 9 ALB. L.J. SCi. & TeCh. 1 (1998)."
[28] "M. A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 Am. J. L. And Med. 591 (2010)."
[29] "Electronic Privacy Information Centre, *IMS Health v. Ayotte*.".
[30] "Sorrel v. IMS Health Inc., 131 S. Ct. 2653 (2011)."
[31] "Vt. Stat. Ann., Tit. 18, §4631 (Supp. 2010)."

First Amendment, and failed the 'heightened scrutiny' test".[32] The Supreme Court further made a statement that if the statute was more straightened privacy based and had made a narrow list where such sale of information is allowed in certain circumstances rather than completely avoiding, then it would have survived the Judicial Scrutiny.[33]

III. INDIAN POSITION: EVOLVING STANDARDS:

III.I RIGHT TO PRIVACY:

The right to privacy in India has taken many turns but irrespective of all those India has joined the US, UK, EU, Canada and South Africa by recognising the Right to privacy as Fundamental right. In Justice ***K. S. Puttaswamy & Anr v. UOI***[34] case, the Supreme Court's nine-judge bench unanimously declared "Privacy is the Constitutional Core of Human Dignity". Chief Justice Khehar borrowing the words of US Supreme Court Justice Louis Brandeis, wrote that "The right to be let alone is a part of the right to enjoy life. The right to enjoy life is, in its turn, a part of the fundamental right to life of the individual." And so it was held that Right to Privacy is a Fundamental Right under Article 21 of Constitution of India.

III.II EXISTING POSITION AND RECENT DEVELOPMENTS:

There are no specific legislations available for the protection of patient's Medical History and Confidential information. Although the Physicians have the obligation to maintain the Confidentiality of his patients because of the Doctor-Patient confidentiality[35] and also disclosing such information will lead to Professional Misconduct as per the Indian Medical

[32] "Id".
[33] "Supra note 30."
[34] "WRIT PETITION (CIVIL) NO 494 OF 2012."
[35] "The Indian Medical Council (Professional Conduct, Etiquette and Ethic) Regulations, 2002 (102 of 1956). ('Medical Council Regulations')"

Council Regulations. But such obligations do exist between any other private or state bodies which do not have any obligation to protect such information. So, there is a high risk of information being misused, thus there is a necessity of separate legislation.

And the first step taken by the Indian Legislature to overcome this crisis was through the amendment of the IT Act, 2000. And the IT Rules which was enacted and introduced in 2011, was the first legislation to explain the term "Sensitive Personal Data"[36]. The rules stipulated the Rights Available for the Information Provider, the rules clearly stated that any corporate bodies or any other persons who obtain sensitive private information for any purpose must obtain Written Consent[37] from the provider of such data and also the data provider must be aware of such data collection and the reason for such collection must also be made known to the provider. And after all the collection of such data should be for a Lawful purpose and in a lawful manner and such purpose should be connected the work carried out by the body or a person.

There are some instances where sensitive information can be made known to the third parties,[38] such as Government agencies that can collect the information for a specific purpose alone but it is subject to the condition that such collection and its purpose should be disclosed to the individual from whom the information is being collected[39] and then when there is a previous contract between the Individual and the body. And then when a body corporate or a person wishes to share the sensitive information, it can transfer such information after the consent obtained and if at all the body corporate or a person who or which receives (Whether inside or outside) the information has the same level of Protection as such as the transferee.[40]

[36] "Information Technology Rules, 2011, Rule 3".
[37] "Information Technology Rules, 2011, Rule 5."
[38] "Information Technology Rules, 2011, Rule 6".
[39] "Information Technology Rules, 2011, Rule 6-proviso".
[40] "Information Technology Rules, 2011, Rule 7".

The person who is in need of information has to simply obtain the written consent from the Data provider under the Indian law further the law does not specify the purpose for which or to which extent the Governmental Discretionary power can be used. Irrespective of all this fair and inadequate laws, the pharmaceutical industries still claim that these limited safeguards will hamper the data collection process. But the pertinent reason behind these rules is International Pharmaceutical Privacy Consortium (IPPC)[41] that deals with the privacy of a patient in pharmaceutical companies. Since Pharma industries are responsible for its products, it requires patient's information with identification in order to know the adverse effects of drugs and this mandates the pharmaceutical companies to keep a tap on patient's drug usage and physician's prescription. And so the IT Rules which requires a written Consent is for the protection of Non-physical damages such as Privacy and Confidentiality.[42]

III.III DISHA (DIGITAL INFORMATION SECURITY IN HEALTHCARE ACT):

This is the first legislative step in India which is completely dedicated to the Protection of Health Information and the Confidentiality of the patient's and the Patient's Right to Privacy of their health information. DISHA Draft Bill was released to the Public domain for comments on 21st March, 2018 by the Health & Family Welfare Ministry of India. India has taken a wider step by enacting a separate legislation for the Health privacy with much more clarity than any other nation because this is the only legislation to appoint authorities at the state level and also the Health information exchange authorities separately for each state and their functions and powers were explained clearly and Data Ownership were provided to the Data subject and the Rights of the Owner has been clearly elucidated alike the EU Directive where the owner has been given the Right to Access, Right to Consent, Right to Refuse, Right to Erasure of information, Right to Rectify, Right to know the place of presence, Right to know the Purpose of Usage of his information are the rights provided to the Right Holder

[41] "International Pharmaceutical Privacy Consortium Comments to Department of Information Technology."
[42] "International Conference on Harmonization (ICH) - Draft Guidance for Industry: E2D Post- Approval Safety Data Management: Definitions and Standards for Expedited Reporting".

under DISHA. And DISHA deals with every problem that arises under this problem confidentiality from the Rights of owner, Appointment–Powers & Functions of the National and State Health authority, to the breaches and Punishment & offences of such breach of Privacy and Confidentiality.[43]

The Act emphasises that any health data including Physiological, Physical & Medical Data, Medical History etc., pertains to a person and any breach amounts to offence and it also states that the owners of the data have the Right to Privacy, confidentiality and Security of their data. And this draft does not allow the commercial exploitation of the health information and do not allow any entities like Insurance companies, Employers, HR Consultancies, Pharma Industries, and any other industries notified by Central Government. DISHA has narrowed down the Rights, Duties and the Access & Exceptions unlike any other legislations all around the world. But the legislation has not yet been passed as the Health ministry awaits the Supreme Court decision on Aadhaar case which involves the issue of Individuals Privacy.[44]

IV. CONCLUSION:

DISHA Draft Bill if passed will be a milestone in this regard, because when the countries like US, UK, EU couldn't make it possible because of the opposition of the Pharma Industries, India would be the only country to make it possible. All the countries have given a wider law with regard to the usage of the Health information and the medical records but DISHA has narrowed down it and has explicitly declared that Pharma industries, Insurance companies or any other entities which use health records for the commercial purpose has been prohibited from such usage and those entities have no rights to access the medical records but this draft also provides an exception clause which exempts the researchers from the commitments. As of now, India does not have any specific legislation on this regard and it depends itself on the

[43] "Digital Information Security in Healthcare Act, Draft for Public Consultation, Ministry of Health & Family Welfare, November, 2017, pg. 4-31."
[44] "Id".

IT Act, 2000, which defines personal information in common and provides for a certain level of protection but does not explain the rights in detail or does not have any penalties for the breaches. It provides for consent clause; however, do not explain the ownership clearly. Even Indian Judiciary has declared the "Right to Privacy" as a Fundamental Right but still, there is no proper set of legislation to prevent the breach of patient's Individual Privacy and the anticipation for the DISHA continues.

It is not only the Indian position but also the position of US and UK are the same as current Indian stand, although they have separate legislation still they could not properly define the term personal information and they couldn't narrow down the rights and control of access and the exceptions to such information. Whereas EU has nearly made it nearer to DISHA Draft by leaving only certain areas, the EU Directive has explained the Rights of the owner in detail but failed to narrow down the Access part and did not speak about the Commercial exploitation in its 2016 Amendment.

Bibliography:

1. Primary Resources:

a) Statutes Referred:

1) *Constitution of India.*
2) *Information Technology Act, 2000.*
3) *Health Insurance Portability and Accountability Act, 1996*
4) *EU Data Protection Directive, 1998*
5) *UK Data Protection Directive, 1998.*

II. Secondary Resources:

a) Articles Referred:

1) *Jeroo S. Kotval, Market-Driven Managed Care and the Confidentiality of Genetic Tests: The Institution as Double Agent, 9 ALB. L.J. SCi. & TeCh. 1 (1998).*
2) *M. A. Rodwin, Patient Data: Property, Privacy & the Public Interest, 36 Am. J. L. And Med. 591 (2010).*
3) *International Conference on Harmonization (ICH) - Draft Guidance for Industry: E2D Post- Approval Safety Data Management: Definitions and Standards for Expedited Reporting.*
4) *Digital Information Security in Healthcare Act, Draft for Public Consultation, Ministry of Health & Family Welfare, November, 2017, pg. 4-31.*
5) *International Pharmaceutical Privacy Consortium Comments to Department of Information Technology.*
6) *N. P. Terry, Symposium: The Politics of Health Law: Under-regulated Health Care Phenomena in a Flat World: Medical Tourism and Outsourcing, 29 W. n Eng. L. Rev. 441 (2007)*
7) *Health Systems governance in Europe: The Role of EU Law and policy 564 (E. Mossialos, G. Permanand, R. Baeten & T. K. Hervey eds., 2010).*
8) *The new EU Regulation on the protection of personal data: what does it mean for patients? A guide for patients and patients' organisations, European Patients Forum (EPF), pg. 1-22.*
9) *Press Association, Tougher Penalties Planned for NHS Data Losses, The guardian (London), and July 1, 2011.*
10) *J. Kulynych & D. Korn, Use and Disclosure of Health Information in Genetic Research: Weighing the Impact of the New Federal Medical Privacy Rule, 28 Am. J. L. And med. 309 (2002).*