PROTECTING PATIENT INFORMATION IN INDIA: DATA PRIVACY LAW AND ITS CHALLENGES

Nimisha Srinivas & Arpita Biswas[*]

Electronic storage of medical records has exposed individuals to the risk of identification at various stages of data collection and data processing. Two options are available to data-miners: to either anonymise information that poses a risk of identification or make such information available to physicians alone. The second option is no longer feasible in a world where the physician-patient relationship is complicated by the presence of other stakeholders, such as insurers and pharmaceutical manufacturers. Finding the proverbial middle path is the only solution to the ethical dilemma posed by the appropriation of patient information for marketing purposes. This paper presents an overview of various data protection regimes, followed by an analysis of the Indian position on data privacy. After the enactment of the 2011 regulations on the processing of personal information under the Information Technology Act, 2000, there is hope that corporations operating in India will comply with international best practices for the fair and lawful processing of personal data.

I. INTRODUCTION

From tracking unauthorized drug prescriptions to assessing the effect of different treatments on patients, the ability to automatically process data provided by thousands of patients has proven invaluable to healthcare service providers globally.[1] It has also become important for healthcare providers to consider patient privacy and data security in the utilization of patient data, especially where such information has stigmatizing consequences.[2]

Rendering information anonymous primarily requires the data controller to filter all personal details from the information provided by data subjects.[3] As a second level of protection, the use of such de-identified information in combination with other information available to the processor should not

---

[*] 5th and 3rd year students respectively, the W.B. National University of Juridical Sciences, Kolkata.

1 M. A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 Am. J. L. and Med. 591 (2010).

2 *See* L. Sweeney, *Patient Identifiability in Pharmaceutical Marketing Data* available at http://dataprivacylab.org/projects/identifiability/pharma1.pdf (Last visited on February 18, 2012).

3 *See* discussion *infra* Part II.B.

reveal the identity of the data subject.[4] In the United States, Part C of the Health Insurance Portability and Accountability Act, 1996 ('HIPAA'),[5] which mandates 'administrative simplification' in the health sector, makes the unauthorized use of *identifiable* personal information punishable.[6] A similar prohibition is contained in the 1995 Council of European Union Directive (the 'EU Data Protection Directive' or 'DPD') on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[7] It is understood therefore that to ensure de-identification of personal data, the data must undergo anonymisation.[8] The degree of anonymity can be ineffective, whereas even de-identified information may sometimes be traced back to the individual.[9] Healthcare providers must therefore ensure an in-built mechanism for patient privacy protection in processing electronic medical records.

Rising administrative costs of data processing in developed countries have resulted in the outsourcing of patient information to under-regulated jurisdictions,[10] where costs are reduced by about half.[11] The dangers underlying the cross-border flow of personal information became apparent in 2003, when a data transcriber in Pakistan threatened to reveal patient information unless the offshoring company, in this case the University of California San Francisco Health Centre, paid her back wages.[12] This was followed by a similar incident in an offshore data processing unit in Bangalore.[13] As examples of data processing gone wrong, these cases were early warning signs of the consequences of a lax data protection regime in India.

It was only last year, however, that the government enacted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('IT Rules'), finally

4 *See infra* text accompanying notes 43-44.

5 Health Insurance Portability and Accountability Act, 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) ('HIPAA 1996').

6 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).

7 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').

8 Rodwin, *supra* note 1, 588.

9 Sweeney, *supra* note 2 (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)).

10 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).

11 *Id*.

12 David Lazarus, *A Tough Lesson on Medical Privacy, Pakistani Transcriber Threatens UCSF Over Back Pay*, S.F. Chron. (San Francisco), October 22, 2003, available at http://articles.sfgate.com/2003-10-22/news/17513957_1_medical-transcription-ucsf-medical-center-medical-privacy (Last visited on February 18, 2012).

13 Terry, *supra* note 10.

effectuating compliance with international standards of data protection.[14] Rules 6, 7 and 8 of the IT Rules, outline disclosure and security requirements in handling sensitive personal data ('SPD'). While the strengthening of India's data protection law has arguably been an inevitable step in the right direction, some of the rules, such as the requirement of written consent from data providers,[15] may seem a bureaucratic nightmare to data processors whose chief concern is cutting costs.

This paper assesses whether the new data protection rules make a difference to patient privacy in India. The rules prohibit the unauthorized transfer of medical records and medical history as misuse of sensitive information.[16] While this may be a blanket prohibition for 'body corporates',[17] state agencies involved in similar data collection activities are given more leeway under the rules. After major security breaches in the UK in 2009 and 2011 involving the loss of tens of thousands of National Health Service ('NHS') patient records,[18] it is clear that the need for privacy-enhancing technologies has increased, particularly within government agencies like the NHS.

Part-II of this paper examines the models of privacy protection evolved in the European Union, United Kingdom and United States and the extent to which these contribute towards protecting patient records. Part-III contains a discussion on the recently introduced IT Rules and the reaction of the pharmaceutical industry to its implications on the handling of SPD in India.

---

[14] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 available at http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15411.pdf (last visited February 18, 2012) ('Information Technology Rules, 2011').

[15] Information Technology Rules, 2011, Rule 5(1) (This provision mandates obtaining written consent from the provider of SPD regarding purpose of its usage).

[16] Information Technology Rules, 2011, Rule 5(2) (This provision prevents collection of information for unauthorized purposes. It states: "(2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless
(*a*) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
(*b*) the collection of the sensitive personal data or information is considered necessary for that purpose").

[17] Information Technology Act, 2000, Explanation to §43A.

[18] *See* Press Association, *Tougher Penalties Planned for NHS Data Losses*, The Guardian (London), July 1, 2011, available at http://www.guardian.co.uk/society/2011/jul/01/tougher-penalties-lost-nhs-records (Last visited on February 18, 2012); *see also* Michael Savage, *NHS "loses" thousands of medical records – Exclusive: Information watchdog orders overhaul after 140 security breaches in just four months*, The Independent (London), May 25, 2009, available at http://www.independent.co.uk/news/uk/politics/nhs-loses-thousands-of-medical-records-1690398.html (Last visited on February 18, 2012).

II. DATA PROTECTION REGIMES IN THE EU, UK AND US

A. THE EU DATA PROTECTION DIRECTIVE

Data protection laws commonly seek to regulate 'personal data' concerning individuals or 'data subjects', handled by both 'data processors' and 'data controllers'.[19] Notably, not all information about a person can trigger the application of data protection law, since only information that affects an individual's privacy can be considered 'personal'.[20] The controller (or the processor designated by the controller to process the data) is responsible for the manner in which a subject's personal data is processed.[21]

The EC Data Protection Directive acts as the basis for various national data protection laws in EU Member States, providing eight data protection principles to the States that apply the Directive.[22] The core data protection principle is the fair and lawful processing of personal information.[23] The information must be obtained for one or more specified and lawful purposes, and must be relevant to the purpose for which they are processed.[24] The data should not be stored for longer than is necessary for the specified purpose.[25] Further, both the controller and processor are under an obligation to enforce appropriate technical and organizational measures to protect against unlawful processing.[26] The processor is subject to the same stringent conditions imposed on the controller, who remains under a further obligation to monitor the processor's compliance with the security measures for the duration of the agency.[27]

---

19 UK Data Protection Act, 1998 (c. 29), §1(1) (This implementing legislation ensures compliance with the data protection principles enunciated in the Data Protection Directive).

20 Durant v. Financial Services Authority, 2003 EWCA Civ 1746 (This case defines data as 'personal' only if it 'affects his privacy'. According to *Durant*, information should be (i) 'biographical in a significant sense' and (ii) second, the focus should be on the data subject, excluding information held by the data controller that contains a passing reference to particular individuals).

21 UK Data Protection Act, 1998, §1(1) (This provision "data controller" means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed).

22 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).

23 UK Data Protection Act, 1998, Schedule 2 and 3 (Conditions for fair and lawful processing of personal data include (i) obtaining the patient's consent and (ii) that data must be processed in the patient's 'vital interests').

24 UK Data Protection Act, 1998, Schedule 1, Part 1, Principles 2 and 3.

25 UK Data Protection Act, 1998, Schedule 1, Part, Principle 5.

26 UK Data Protection Act, 1998, Schedule 1, Part I, Principle 7 (Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data).

27 P. ROOM & F. F. WATERHOUSE, BUTTERWORTHS DATA SECURITY LAW AND PRACTICE 68 (2009).

The Directive also lays down a general presumption against the adequacy of data protection laws in third countries.[28] Where transfer of data takes place between States that have enforced the Directive by implementing similar domestic laws, the data controller (who is in possession of the information) can be confident that the level of protection offered in the recipient country matches that in the host State.[29] Where transfer of data takes place between a Member State and a third country, however, the adequacy of protection offered by the third country will be evaluated in light of surrounding circumstances, such as nature of data and purpose and duration of the proposed processing operation.[30]

The European Court of Human Rights ('ECtHR') emphasized the importance of protecting a person's health data in *I* v. *Finland* in 2008.[31] The case involved an employee of an eye clinic, formerly a patient at the clinic, whose HIV status became known to her colleagues due to free access to the patient register containing information on diagnoses and treatment.[32] The ECtHR noted in the case that the "sensitive issues surrounding this disease" would make the requirement of confidentiality particularly important in the applicant's case.[33] This observation of the ECtHR places an obligation on data controllers to keep all confidential data safe from unauthorized access.[34]

B. COMMON LAW POSITION UNDER THE UK DATA PROTECTION ACT, 1998

Ordinarily, anonymized information should not present much of an ethical dilemma to healthcare professionals. The mere de-personalisation of patient data, however, does not offer sufficient justification for decreasing the level of protection ordinarily afforded to personal data.[35] Personal data is defined under §1(1) of the DPA as "data which relate to a living individual who

---

28 Data Protection Directive, Arts. 25 and 26.

29 Health Systems Governance in Europe: The Role of EU Law and Policy 564 (E. Mossialos, G. Permanand, R. Baeten & T. K. Hervey eds., 2010) ('Health Systems Governance in Europe').

30 *Id.*

31 *See* I v. Finland, Application No. 20511/03: 2008 ECHR 623 (The ECHR stated (upholding the Court's previous decision in Z v. Finland, (1988) 25 EHRR 371) that the protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the European Convention on Human Rights. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention).

32 Room & Waterhouse, *supra* note 27, 51.

33 *Id.*

34 *See supra* note 31.

35 Beyleveld, D. & Histed, E., *Case Commentary: Anonymisation is Not Exoneration*, (1999) 4 Med. L.I. 69 73-74 *cited in* Principles of Medical Law 658 (A. Grubb, J. Laing & J. McHale eds., 2010) ('Principles of Medical Law') (For example, a woman who is a devout Catholic may be opposed to the use of her data in research for chemical contraceptive methods).

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 not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."[36] Therefore, it is evident that the test for de-personalisation of data must involve more than mere anonymisation of the data.

The question of whether the use of anonymized patient data is a breach of patient privacy was examined by the Court of Appeal in *R* v. *Department of Health, ex p Source Informatics*.[37] A data collection company, in this case, wished to sell anonymised data collected from pharmacists to ascertain the prescribing habits 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 reasonably expectation of privacy is limited to primary uses of identifiable information.[38] Primary uses could conceivably include the updating of a hospital's record of a patient's medical history or the pursuit of specific research objectives, for which the prior consent of the data subject has been obtained. The view taken in *Source Informatics* appears to be out of line with the expansive interpretation of an individual's private life in a recent decision of the ECtHR.[39] The ECtHR understood the concept of 'private life' broadly to include a person's name, family life and information about a person's health, thereby protecting a person's right to control all aspects of his life.[40]

§11 of the UK's Data Protection Act, 1998 ('DPA') entitles an individual to notify the data controller to cease processing 'for the purposes of direct marketing' any personal data of which he is the data subject. Although the argument was not considered in *Source Informatics*, data subjects, whose information was being anonymised and then commercially exploited by the data collection company, should have been notified as to the purposes of anonymisation.[41] Further, since §1(1) of the DPA defines 'processing' as 'adaptation or alteration', patients whose data is being anonymised are entitled to notification by the data controllers about the purposes of such 'processing' under the second data protection principle.[42]

It is dangerous to assume however that anonymization of data removes the obligation on the data controller to comply with data confidentiality

---

36 Data Protection Directive, Recital 26.
37 (1995) 4 All ER 185, rev'd (2001) QB 424 (CA) ('Source Informatics').
38 *Id.*; Principles of Medical Law, *supra* note 35, 659.
39 S and Marper v. UK, (2009) 48 EHRR 50, ¶ 66-67.
40 *Id.*
41 Principles of Medical Law, *supra* note 35, 707.
42 *See supra* note 19.

laws. In *Common Services Agency* v. *Scottish Information Commissioner*,[43] the disclosure of information relating to the incidence of childhood leukemia in particular neighbourhoods was refused by the Common Services Agency, citing a high risk of identification due to the low incidence of individuals suffering from the condition in those areas. The House of Lords held that the anonymised information should be sufficiently de-personalised before disclosure,[44] remitting the application to the Information Commissioner for consideration in view of the above decision.

Under the *Source Informatics* standard, the use of patient-identifiable information is absolutely prohibited.[45] This standard does not address concerns over secondary uses of anonymised information, where the effect on the data subject's private life is unclear. At the other end of the spectrum is the ECtHR's rights-centric approach, which could have the effect of imposing prohibitively high costs on today's globalised healthcare industry. A more practical approach would ensure that data collectors employ transparent methods of collection, processing and storage.

C. UNITED STATES POSITION: THE DANGERS OF PHARMACEUTICAL MARKETING

In the US the HIPAA aims to improve "the efficiency and effectiveness of the healthcare system by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information."[46] Patient privacy can be ensured at various stages of information collection, processing and disclosure.[47] Information that is de-identified at the stage of collection may serve the purpose of preserving patient anonymity. Further, the range of justifiable reasons for collection of personal data may be limited to certain purposes alone, such as treatment.[48] Therefore, informational privacy guarantees that the information is not disclosed to corporate entities. As healthcare delivery systems evolve and the physician-patient relationship becomes more complicated, however, other interested stakeholders are now gaining a stronger foothold in

---

43 (2008) UKHL 47.

44 *See* Principles of Medical Law, *supra* note 29, 693 (For the anonymised information to be considered 'personal' (per S. 1(1) of the Data Protection Act 1998), and therefore protected by the data protection principles, the data controller or CSA should be able to connect the anonymised data to any other information in its possession (like the original statistics) in order to identify the individuals involved)).

45 Health Systems Governance in Europe, *supra* note 30, 564.

46 HIPAA 1996, §261.

47 Terry, *supra* note 10, 3.

48 *Id*.

the healthcare industry.[49] With commercialization on the rise, the balance now tilts in favour of service providers' gaining access to patient information.[50]

The concern over aggregation of patient information does not appear to be overstated in view of the absence of strict requirements of consent under the HIPAA. The market for patient data is growing worldwide.[51] Apart from the Food and Drug Administration in the US, health insurers, researchers and drug manufacturers are actively using prescription information commercially.[52] It is not surprising therefore that various state governments have failed to defend legislation preventing the sale of prescription data to pharmaceutical companies against challenges by data mining companies that such laws violate their First Amendment rights.[53]

With the Supreme Court striking down a prescription confidentiality law in Vermont in early 2011, a free rein has been given to corporates in America to potentially abuse patient disclosures.[54] Vermont had enacted restrictions, both on the nature of information as well as on who was allowed to use information for marketing purposes, which pharmaceutical manufacturers claimed were violations of their free speech rights.[55] Since the state was unable to show that the statute directly advanced a 'substantial government interest', however, it was held by the Court that the content-based burden in §4631(d) of the Vermont statute affected expression protected under the First Amendment, and failed the 'heightened scrutiny' test.[56] The Supreme Court recommended that a statute which was more protective of privacy or which permitted the sale of information in only a few narrow and well-justified circumstances might have survived judicial scrutiny.[57]

---

49 *See* 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) (Managed care, a modern-day healthcare delivery structure, represents the streamlining of clinical care with a special emphasis on cost-effectiveness. A fall-out of this model of healthcare is the decreasing importance given to confidentiality of medical records, including genetic records, in favour of cutting costs and bypassing patient consent).

50 Terry, *supra* note 10, 3.

51 *See* Rodwin, *supra* note 1, 592 (IMS sells data for marketing in over 100 countries and earned over $ 2 billion in 2006).

52 *See* Health Systems Governance in Europe, *supra* note 29, 578.

53 Electronic Privacy Information Centre, *IMS Health v. Ayotte*, available at http://epic.org/privacy/imshealth/ (Last visited February 18, 2012) (Maine, Vermont and New Hampshire are among several states that enacted laws to curtail the marketing of patient-identifiable prescription data).

54 Sorrel v. IMS Health Inc., 131 S. Ct. 2653 (2011).

55 *Id.*, 2.

56 Vt. Stat. Ann., Tit. 18, §4631 (Supp. 2010).

57 Sorrel v. IMS Health Inc., *supra* note 54, 3.

III. INDIAN POSITION: EVOLVING STANDARDS

No specific legislation regarding the disclosure of medical records exists in India. Under the Indian Medical Council Regulations, however, every medical professional is obligated to maintain physician-patient confidentiality.[58] While a physician disclosing personal information about his or her patients could be held guilty of professional misconduct,[59] this obligation does not extend to other persons responsible for processing patient data,[60] either under the mandate of a state body or a body corporate. Physicians are only allowed to disclose patient information to public health authorities in limited circumstances, such as in case of a 'serious and identified risk to a specific person and/or community'.[61]

A. RIGHT TO PRIVACY IN INDIA

Contrary to the trend in the UK and US, the Indian judiciary has carved out the right to privacy as an exception to the rule that permits interference by public authorities in an individual's private life.[62] The Supreme Court has on several occasions emphasized that the right to privacy is not an absolute right.[63] Instead, the Court has chosen to adopt a case-by-case approach in the interpretation of the right to privacy.[64] There have been instances where the Court has allowed a hospital to inform the patient's future spouse about his HIV positive status.[65] The rationale for disclosure in such cases has been the public welfare argument that the negligent spreading of an infectious disease

---

58 The Indian Medical Council (Professional Conduct, Etiquette and Ethic) Regulations, 2002 (102 of 1956). ('Medical Council Regulations').

59 Medical Council Regulations, Chapter 8 (Disciplinary action may be taken against physicians for any offences committed in violation of the regulations).

60 Medical Council Regulations, Rule 1.1 ('Character of Physician' covers only "Doctors with qualification of MBBS or MBBS with post-graduate degree/diploma or with equivalent qualification in any medical discipline" are covered under the Regulations).

61 Medical Council Regulations, Rule 7.14.

62 Aparna Vishwanathan, Outsourcing to India: Cross Border Legal Issues 318 (2008).

63 *See* Sharda v. Dharmpal, AIR 2003 SC 3450 ("Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right, such fundamental right must be subject to restriction on the basis of compelling public interest." The petitioner had had an abortion and refused to be subject to a DNA test ordered by the Court, at the instance of her husband. The Court did not recognize the petitioner's right to privacy in this matter, citing public interest); *see also* Selvi v. State of Karnataka, (2010) 7 SCC 263; Ms. X v. Mr. Z, 96 (2002) DLT 354.

64 *See* Govind v. State of Madhya Pradesh, AIR 1975 SC 1378 (The Court stated that, "The right to privacy in any event will necessarily have to go through a process of case-by-case development").

65 Yepthomi v. Apollo Hospital Enterprises Ltd., AIR 1999 SC 495; Mr. 'X' v Hospital 'Z', (1998) 8 SCC 296.

is an offence against public safety.[66] This approach, which construes individual autonomy only in the context of whether or not an interface with public interest exists, differs considerably from the ECtHR's rights-centric approach in *I* v. *Finland*.[67]

In resolving the clash between the 'right to be let alone' and the 'greater good' of the public, the judiciary has leaned towards favouring public interest over individual privacy.[68] In *Sharda* v. *Dharmpal*, a husband filed for divorce on the basis that his wife was mentally ill.[69] In order to prove this fact, the wife was compelled to undergo a medical examination. She claimed that being forced to do so without her consent would be violative of her personal liberty. After stating that the 'right to privacy' is not an absolute right, the Court held that the absence of such data would make it impossible to reach a decision on the facts of the case.[70]

In *Shri G.R. Rawal* v. *Director General of Income Tax (Investigation)*,[71] the bench discussed the ambit of §8(1)(j) of the Right to Information ('RTI') Act, 2005, which excludes disclosure of 'personal information' in response to an application.[72] The Central Information Commission, however, held in this case that the exclusionary rule would not apply where the larger public interest justifies disclosure.[73] Citing a 2007 decision of the Bombay High Court where the Court allowed disclosure of a prisoner's medical condition in response to an RTI application,[74] it was further stated that a determination of justifiable disclosure would be made on a case-to-case basis. While there may be exceptional circumstances that justify disclosure in public interest in some cases, the judicial trend observed in these cases has led to a gradual erosion of the principles of personal liberty, autonomy and privacy. Clearly, the

66 Indian Penal Code 1860, §269, (Non-disclosure of HIV+ status may be considered an offence, 'Negligent act likely to spread infection of disease dangerous to life').

67 *See supra* note 31.

68 Sharda v. Dharmpal, AIR 2003 SC 3450.

69 *Id.*

70 *Id.*

71 No. CIC/AT/A/2007/00490 (decided by Central Information Commission on March 5, 2008) ('G.R. Rawal').

72 *Id.* ("§8(1)(j), therefore, excludes from disclosure an information which relates to personal information the disclosure of which
(*i*) has no relationship to any public activity or interest; or
(*ii*) would cause unwarranted invasion of the privacy of the individual").

73 *Id.* ("An invasion of privacy may also be held to be justified if the larger public interest so warrants").

74 Mr. Surupsingh Hrya Naik v. State of Maharashtra through Additional Secretary, General Administration Deptt., AIR 2007 Bom 121 ("If patients are to be admitted in hospital for treatment then those employees in the hospital are duty bound to admit only those who are eligible for admission and medical treatment. The records of such institution, therefore, ought to be available to Parliament or the State Legislature. The Parliament/Legislature and/or its Committees are entitled to the records even if they be confidential or personal records of a patient. Once a patient admits himself to a hospital the records must be available to Parliament/ Legislature, provided there is no legal bar").

Supreme Court's case-by-case approach to defining privacy does not provide the kind of safeguards that are available under a strong data protection regime, which respects individual autonomy.

Even more controversially, the Court has ruled that information contained in a public record cannot be protected under the right to privacy.[75] Since public records could include hospital records, prison records, and any other information collected by a state body, this ruling may have the effect of bypassing any authorization requirement of collecting patient data already contained in public records. It is important, therefore, that a comprehensive data protection law is enacted to regulate the flow of information in the hands of the State.

B. RECENT DEVELOPMENTS

The Information Technology Act, 2000, has had several amendments in the last couple of years that have expanded and changed the law according to the latest technological innovations. The IT Rules introduced in 2011,[76] define 'sensitive personal data' for the first time in India.[77] The Rules stipulate that a body corporate collecting such sensitive personal data shall obtain written consent from the provider of said data.[78] This data can only be collected for a lawful purpose, which is connected to the working of the body corporate. The body should also make sure that the data provider is made aware of the fact that such information is being collected. The provider should be made aware of the reasons for which such information is being collected and of the identity of the persons who intend to receive such information.[79]

There are very few instances in which sensitive personal data can be disclosed to a third party, such as when under a previous contract, the provider has consented to such disclosure by the body corporate.[80] Government agencies can collect such information without prior consent, subject to the condition that the information is collected for certain specified purposes alone and that those purposes are made known to the individual.[81] The only basis on

---

75 Mr `X' v. Hospital 'Z', (1998) 8 SCC 296.

76 Information Technology Rules, 2011, *supra* note 14.

77 Information Technology Rules, 2011, Rule 3 (Sensitive Personal Data includes information relating to the physical, physiological and mental health condition, sexual orientation, medical records and history and biometric information of an individual).

78 *Id.*, Rule 5; *see also* UK Data Protection Act, 1998, §7(2).

79 UK Data Protection Act, 1998, §§7(1)(b)(ii) & (iii) (This provision contains a similar requirement).

80 *See* Information Technology Rules, 2011, Rule 6 (While prior permission of the data provider is required under this rule for disclosure of SPD, §55 (2)(a)(ii) of the Data Protection Act, 1998, requires the consent of the data controller for either obtaining or disclosing personal data).

81 Information Technology Rules, 2011, Proviso to Rule 6.

which a body corporate in India can send data to other such bodies (whether within or outside India) is if they maintain the same level of data protection.[82]

In 2008, §43A was introduced through the Information Technology (Amendment) Act, 2008, to hold a 'body corporate' liable for any negligence in the implementation or maintenance of reasonable security practices and procedures.[83] In case any person had wrongfully suffered a loss, the body corporate would be legally responsible to compensate the person by way of damages.[84] Rule 8 of the IT Rules also imposes a duty on the body corporate to ensure compliance with practices and procedures in securing personal information. Additionally, these practices must incorporate 'managerial, technical, operational and physical security control measures' that are adequate to the kind of information assets being protected.[85]

While the Data Protection Directive specifies narrow circumstances that justify the use of SPD, the Indian rules simply require the obtaining of written consent from providers of information. Further, the blanket provision allowing the Government to collect information without the consent of the provider does not specify the purposes for which its discretionary power may be used. Despite the fairly diluted standard of data protection that has been incorporated in the IT Rules, there have still been objections from lobbyists for pharmaceutical companies on the ground that the limited safeguards within the Rules that prevent misuse of SPD will hamper the process of data collection.

One of the main lobbyists for this position is the International Pharmaceutical Privacy Consortium (IPCC), which deals with the promotion of sound policies for patient privacy in pharmaceutical companies that have operations in India.[86] Their position is that pharmaceutical companies are responsible for the safety of their products, which require them to provide patients with identifiable information in dealing with reports regarding adverse reactions to drugs. It is imperative, therefore, for these companies to continue collecting personal health data to ensure proper application of safety measures. If the recommended good practices for pharmaceutical companies were to be properly implemented, such companies would have to keep track of information about patients using the drug and physicians prescribing them.[87] Additionally, as per

---

82 Information Technology Rules, 2011, Rule 7.

83 Information Technology (Amendment) Act 2008, No. 10 of 2009, available at http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf (Last visited on February 18, 2012).

84 *Id.*

85 Information Technology Rules, 2011, Rule 8.

86 International Pharmaceutical Privacy Consortium Comments to Department of Information Technology, available at http://www.pharmaprivacy.org/download/IPPC%20Comments%20on%20Information%20Technology%20Rules%202011.pdf (Last visited on August 17, 2012) ('IPCC Comments').

87 *Id.*, 2.

the regulatory requirements governing US companies operating in India, following up with patients on the effects of the drug is mandatory, which requires them to retain a patient's SPD in order to perform these follow ups.[88]

According to the IPCC, the IT Rules could bring to a halt important biomedical research that involves personal health data.[89] Even though it is largely undisputed that consent is important to prevent physical harms, they argue that it is now being used to prevent non-physical harms like privacy and confidentiality.[90] Biomedical research largely consists of 'key-coded'[91] data. This data is mainly stored in order to facilitate additional research purposes in the future.[92] Since secondary research branching out from the primary research cannot be determined during the first stage,[93] researchers will have to obtain private medical information relating to the patients. Such information should, however, be de-identified as researchers do not specifically need to know the identity of the patient group.[94] It is anticipated that the Rules may substantially hamper this process because it would require companies to get in touch with the patients to obtain their consent. This may even lead to a reduction in the number of consenting patients, even if they know that the information being provided will be partially de-identified. Notwithstanding the obvious relevance of ethics in these situations, the principles of data protection and patient privacy should factor in biomedical research as an important permitted use.

Currently, the Indian lobby for pharmacovigilance (the study and prevention of adverse effects of a drug) like the IPCC consists mainly of conglomerates in the pharmaceutical industry. They advocate the use of partially de-identified information towards advancing medical research that could lead to the discovery of novel treatments. Their support for the use of pseudonymised (or partially de-identified) information could, however, lead to an erosion of the principles of data privacy.

IV. CONCLUSION

In the US, the debate has acquired an added dimension – whether pharmaceutical companies may collect patient information for secondary purposes such as marketing. Companies have defended the use of sensitive prescription information for marketing purposes as a part of their right to commercial

---

88 International Conference on Harmonization (ICH) - Draft Guidance for Industry: E2D Post-Approval Safety Data Management: Definitions and Standards for Expedited Reporting *available at* http://www.fda.gov/RegulatoryInformation/Guidances/ucm129457.htm (Last visited on August 17, 2012).

89 IPCC Comments, *supra* note 84, 3.

90 *Id.*

91 *Id.*

92 *Id.*, 4.

93 *Id.*

94 *Id.*, 2.

free speech under the First Amendment. As discussed earlier, the debate in the US has by no means been settled by the recent Supreme Court decision in *Sorrel* v. *IMS Health Inc*, which struck down a prescription confidentiality law in Vermont. Arguably, prescription confidentiality laws are necessary to protect patient privacy in the absence of any requirement of authorisation in the HIPAA for secondary uses of information. While it is easy to justify data collection by pharmaceutical companies for primary purposes such as biomedical research, which are subject to an authorization requirement under the HIPAA, patient information may be used for secondary purposes like marketing without the consent of the data provider. At least in principle, therefore, there is a strong case to be made for supporting patient privacy over public interest in advancing biomedical research.

The framework for data protection offered by the IT Rules does not provide an exhaustive list of the permitted purposes for which SPD may be used. Further, the wide powers of data collection that have been vested in the State, which are constrained only by a 'communication of purpose' requirement, may result in situations akin to the leaks involving the NHS database in the UK. The most comprehensive standard in the present scenario appears to be the Data Protection Directive, which identifies the data protection principles that form the basis of national data protection laws among EU member states. The Data Protection Directive is also evidence of a strong regulatory framework that restricts the power of third parties, including government bodies, to collect SPD.

Admittedly, the effect of introducing the concept of 'sensitive personal data' to the IT Rules in India is yet to be determined. It is likely that the enforcement of these new standards will be determined in line with the 'right to privacy' jurisprudence developed by the courts in India. However, it is hoped that since the amendments reproduce verbatim the UK Data Protection Act, which enforces the Data Protection Directive, the courts will consider both common law and ECHR jurisprudence in protecting patient-identifiable information.