

## The Impact of Data Privacy Protection in Medical Practice in Singapore

Tay Sun Kuie MD, MAppLaw

Department of Obstetrics and Gynaecology, SGH

### ABSTRACT

The 1995 European Community Directive on Data Privacy provides a legal framework for data collection and processing. The directive specifies that data collection must be fair and lawful, adequate, relevant and with the patient's informed consent. Data must be kept for not longer than necessary and be processed for the intended purpose. Patients should have the right to access the data to confirm if the data and type of data on them are correct and up-to-date. With appropriate justification, they have the right to rectify, erase or block certain data from being processed or collected. The data is prohibited from being transferred to other countries without adequate data privacy protection unless there is a contractual obligation. The directive has been enforced in a number of countries such as the United Kingdom in its Data Protection Act 1998.

In Singapore, personal privacy and privacy of medical data are protected by common law and statutes, including the Computer Misuse Act 1998 for electronic data. Code of ethics and guidelines for good clinical practice call for assurance of the quality of data. These are not legally enforceable. There is no provision for patient's right of access or objection to the data, nor protection of data from secondary processing and transfer to other countries.

The rising incidence of offences for unauthorised access to data under the Computer Misuse Act 1998 suggests that violation to data privacy in Singapore is more prevalent than generally acknowledged. The hitherto unspoken issues on data privacy may assume a much higher profile in the near future. Even though domestic demand for legislation on data privacy maybe low now, the changed environment internationally may be a strong push for Singapore to take a closer look at the role of data privacy legislation in order to remain competitive globally.

*Keywords:* code of practice, common law, data processing, statutes, transborder data transfer

### INTRODUCTION

Medical confidentiality is a long held professional obligation in doctor-patient relationships. It allows a doctor access to many aspects of a patient's privacy, including details on his illnesses and sensitive personal information on demography, socio-economic state, recreational habits, and religious and sexual practice. There is a growing public concern on the potential erosion of patients' personal privacy.<sup>1</sup>

The problem of patient's privacy is more acute now than ever partly because of the wide adoption of electronic data collection systems in healthcare systems. Compared to the laborious traditional manual records which are necessarily brief, often incomplete and fragmented, recent advances in information technology provides huge electronic data storage capacity which facilitates a vast variety of data to be collected easily

and captured for a long time cheaply. Not surprisingly, there is a massive proliferation of medical databases for clinical management, research and compilation of important epidemiology statistics. Consequent to the rapidly increasing utilisation of electronic communications such as e-mail, the Internet and telecommunications, personal data, sometimes in large volumes, are being transmitted between various parties located in different parts of the world.<sup>2</sup> The improved patient satisfaction and patient education brought about by the information technology revolution also open the floodgates for breaches in upholding a patient's privacy.<sup>3,4</sup>

The 1995 European Community Directive on Data Protection called upon the member states of the Union to enact national laws on personal data protection for privacy, including data collected in medical practice and healthcare management.<sup>5</sup> This calls for the issue

of data privacy in medicine to be closely examined. This article examines the impact of medical data privacy protection on medical practice in Singapore.

## DATA PRIVACY

The issues on patient's privacy in healthcare systems dominated by information technology today are related to patient identities in publications and access to patients' medical records by a third party i.e. a patient's wish to limit the disclosure of personal information.<sup>6,7</sup> For example, the New Hampshire psychiatrist who repeatedly looked at the medical records of an acquaintance without permission was held guilty of intruding into a patient's privacy.<sup>8</sup> In a 1999 survey by the California HealthCare Foundation, one in five American adults believed that a healthcare provider, insurance plan, government agency or employer had improperly disclosed personal medical information.<sup>9</sup> Half of these people believed that it resulted in personal embarrassment or harm. In 2000, a Gallup survey for MedicAlert Foundation found that 77% of the respondents said that the privacy of their personal health information was very important and that 61% were very concerned that their personal health information might be made available to others without their consent.

Many people fear that health information maybe used against them in denying them insurance, employment, housing or credit application; or in exposing them to unwanted judgement or scrutiny. Others feel that a breach of a patient's privacy can harm the patient's personal safety, and cause financial loss and disruption of activities.

A breach of privacy can also damage the reputation and goodwill of the doctor, clinic, hospital or healthcare organisation. More importantly, there maybe loss of public confidence in the organisation, and this may give rise to litigation for failure to meet legal obligations.

## THE EUROPEAN COMMUNITY DIRECTIVE ON DATA PROTECTION 1995

"Personal data" was defined in the European Union (EU) Directives as any information concerning an identified or identifiable person, such as an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. The processing of personal data is defined as any operation with personal data, which may or may not involve automatic means. It includes collection; recording; organisation; storage; adaptation; retrieval; consultation; use; disclosure by

transmission; dissemination or otherwise making available; alignment or combination; blocking; and erasure or destruction of data. There are 7 issues pertinent to healthcare practice and management which warrant closer scrutiny, analysis and discussion.

### *Category of Personal Data*

Personal information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life are considered highly personal and sensitive information. Their collection is generally prohibited except when data processing is required for the purpose of preventive medicine, medical diagnosis, provision of care or treatment, or management of healthcare services. Collection, however, requires explicit informed consent from the subject.

### *Data Quality*

The quality of data must be assured. They must be obtained and processed fairly and lawfully; held and processed only for specific, explicit and legitimate purposes; adequate, relevant, and not excessive; accurate, complete, and where necessary, up-to-date; and held no longer than necessary.

This poses a particular difficulty in medical practice as some data would be invaluable for epidemiological research of public interest some decades later. Initiatives to improve patient management often rely on audit of past treatment experience of sufficient duration. It is therefore not possible at the time of data collection to inform the patients of the duration of data storage and possible future usage of the data.

### *Informed Consent*

Data collection is legitimate only if the subject gives an unambiguous informed consent of the existence and purposes of the operation and the duration of data storage. If the data is considered for passing to third parties, the data subject must be informed of the potential third parties and their anticipated processing of the data.

### *Right to Access to Data*

A subject has the right of access to data collected on him at a reasonable interval regarding confirmation on whether his data has been processed and of the purpose of processing, category of data collected, and recipients or category of recipients to whom the data are disclosed.

The subject is also guaranteed rectification, erasure or blocking of data processing where there is non-

compliance with the provisions of the Directive or where the nature of the data is incomplete or inaccurate. It also allows the patient to endorse locking of certain sensitive information, such as psychiatric assessment and serology test result for the human immunodeficiency virus, to some healthcare providers.

### ***Right to Object Processing of Data***

A subject has the right to object data processing if there is compelling justification or if data is processed for the purpose of direct marketing or if the data is used by a third party for direct marketing.

Medical information is becoming more fluid and more easily available online. Commercial interests are becoming more sophisticated in the selling and sharing of that information. Senator Patrick Leahy, sponsor for the American Medical Information Privacy and Security Bill in 1996, cited a case of a man who had a diagnosis and treatment for depression and who then found his name on a solicitation list for sales literature for Viagra, a drug used to treat men with sexual impotence.<sup>10</sup> The disclosure of medical data to marketing agents could give rise to great personal distress and embarrassment in the data subject. It is a basic principle of privacy for anyone to have a right to object processing of his or her medical data if the purpose of processing of the data includes a possibility of disclosure to a third party with an intention of direct marketing.

The right to object medical data collection is limited. For personal data collected lawfully on grounds of public interest, official authority or the legitimate interests of a natural or legal person, a subject has a right to object the data related to him from being processed only when there are legitimate and compelling reasons specific to his circumstances. Medical databases and registries, such as a national cancer registry which serves to provide trends in incidence of cancers and changes in factors contributing to cancers, are necessarily as complete as possible in the inclusion of all the cancer patients for accurate interpretation of data analysis and conclusion. Patients' self-selection for exclusion to the data processing may bring biases which negate the purpose, wholly or substantially, of the registry. The Directive provides Member States to lay down national provisions contrary to this right to object processing of data.

### ***Confidentiality and Security***

The confidentiality and security of patients' data are protected from unauthorised, either intentional or

unintentional, access or disclosure of the patient's identity to a third party. The EU Directive recommends for a Controller, who is the person, or public authority or agency, to determine the purposes and means of the processing of personal data.

The issue of access to a patient's medical information is a thorny clinical management problem. Increasingly, healthcare delivery to a patient involves a number of healthcare providers at different levels of expertise. Medical information is transferred to various locations where the caregivers carry out their duties. The probability for breaching the patient's confidentiality can be minimised by a well designed computerised medium of data transfer, meticulously confirming the identification of patient and the requestor's identity and his need to know the data.<sup>11-14</sup>

Patient anonymity is an important measure to prevent disclosure of a patient's identity. However, it does not allow verification of reports and existence of data-subject in prevention of scientific errors and frauds. Some cases or records may be duplicated inadvertently. Patient identity is required for follow-up study if more evidence is needed, verification of consent and surveillance of consequence of research intervention.

### ***Transfer of Data to Third Countries***

Personal data can be transferred to third countries where there are provisions for personal data protection equivalent to the Directive. For a legitimate transfer of personal data to a third country without legal provision for personal data protection, the third country must ensure adequate level of protection judged by all circumstances surrounding a data transfer operation and by special consideration of the nature of the data, the purpose and duration of the proposed processing operation, the country of origin, and country of final destination. In addition, the subject must give an unambiguous consent for the transfer.

It is envisaged in the provisions of the Directive that transferring of data across a country's border within the EU will be free and easy as the member states are required of enacting equal legislation to protect personal data. In contrast, transferring personal data from the EU to another country without a privacy or data protection laws is prohibited, unless the recipient country can make provision of data protection equal to that of the host country. In 1999, the Group-8 reported that it was the protection of personal health information that was the most significant barrier to the formation of a Global Information Society for Health.<sup>15</sup> Other international organisations, such as the Organization for Economic Co-operation and

Development, may play a pivotal role in providing a model law on data protection in transborder flows of medical information.<sup>16</sup>

## PRIVACY IN SINGAPORE

Singapore does not have a privacy law or personal data protection law. Issues concerning the right to privacy and protection of personal data, particularly medical data, are addressed by common law, legislatures and Code of practice.

### *Common Law*

In common law, the law of confidence protects the confidentiality or secrecy of information based on 3 criteria:<sup>11</sup>

1. the information itself must have the necessary quality of confidence about it;
2. the information must have been imparted in circumstances importing an obligation of confidence; and
3. there must be unauthorised use of that information to the detriment of the party communicating it.

Protection can last forever if the information remains “confidential”. However, protection ceases once the information is no longer a secret.

In the law of tort, “...there is a general duty not to cause foreseeable harm to another ...A patient may file a negligence suit if there is any unauthorised disclosure of confidential information about him that causes him damage”.<sup>7</sup> Therefore, a doctor must think carefully before disclosing information about his patient and should restrict information to those who need to know, including communication between the employer and the doctor treating an employee. By obtaining a patient’s consent on disclosure of information relating to him and allowing him the right to object to it, doctors will obviate any legal liabilities.

### *Statutory Legislation*

There are more than 150 laws with privacy provisions in Singapore. Some of them specifically related to healthcare, while others are for general application.

#### *Statutory Control of Medical Information*

### **Data Collection**

Apart from clinical information that physicians collect in the course of medical management and those that administrative personnel collect for administration,

there are some data that are collected under statutory requirements.

The 1985 Termination of Pregnancy Act (Cap324) requires that the name, obstetric history, marital status and educational level of the woman be collected and forwarded to the Ministry of Health.

The Ministry of Health Guidelines on Human Embryology and The Practice of Reproductive Technologies in Singapore, 1994 require all children born by in-vitro fertilisation technologies to be registered. The identity of the children is coded by their birth certificate number.

### **Data Disclosure**

Under the Infectious Diseases Act (Cap 137), every doctor has a duty to disclose medical information by notifying the director of medical services if he believes a patient is suffering from an infectious disease. Every person in charge of a laboratory used for the diagnosis of disease who becomes aware of an infectious disease must also give notice to the director. Failure to notify is a criminal offence. The Act provides exceptions to medical confidentiality on information identifying persons with AIDS or sexually transmissible diseases (STDs). Any person who is aware that another person has AIDS/HIV infection or a STD cannot disclose any information that identifies the person except:

1. with the person’s consent
2. when the court orders
3. to any doctor or healthcare staff treating the person
4. to any blood, organ, semen or breast milk bank where the person is a donor
5. to the victim of the person’s sexual assault
6. to the Controller of Immigration
7. to the next-of-kin upon the person’s death
8. to any person, where in the opinion of the director of medical services, it is in the public interest.

Under the Infectious Diseases Act, a doctor may disclose information of an infected person to the spouse, former spouse or any other contact of the infected person, or to a health officer to disclose to any of these parties, if the doctor reasonably believes that:

1. it is medically appropriate and there is a significant risk of infection to the other parties;

2. the infected person will not inform the other parties accordingly, after counselling on the need to notify them;
3. he has informed the infected person of his intention to disclose the information.
4. he is reasonably unable to counsel or inform the infected person and applies to the director of medical services for waiver to counsel and inform.

### **Informed Consent**

There is no comprehensive statutory requirement for patients to consent to data collection. Large databases exist for cancer registry, birth defect registry, thalassaemia registry, for example.

### **Right of Access and Right to Object to the Data**

There is no statutory protection of a patient's right to access to the data collected on them for confirmation of accuracy and rectification, or for objection. As informed consent is not required, some patients may not be aware of the existence of the data collection.

### **The Computer Misuse Act (Cap 50A) 1998**

The Act defines several offences related to unlawful use of computers. Its scope covers all types of computers and any information stored, processed or transmitted with computers. As the Singapore healthcare systems increasingly utilise computers, engage more computer software, and create more databases, the impact of this Act also becomes more relevant and evident. Under the Act, any person engaged in any unauthorised access to any programme or any data in the computer, or modification to computer material, either temporarily or permanently, regardless of the type of programme or data in the content is deemed to have committed an offence. It is also an offence for any person who, knowingly and without an authority, discloses the access code, password, or any other means of accessing a computer, if his action was for any wrongful gain, or for any unlawful purpose, or for causing any wrongful loss to any person.

In a keynote address on the Subordinate Court 10th Workplan, 2001, the Honorable Chief Justice of Singapore reported the number of people convicted under the Computer Misuse Act had increased from 14 in 1996 to 191 in 2000. The number of cases of unauthorised access under Section 3 increased from an average of 4 to 5 cases a year between 1996 and 1998 to 12 cases in 2000. The number of cases convicted under Section 5 for unauthorised

modification of the contents also increased from an average of 5 cases between 1997 and 1999 to 8 cases in 2000.

### **Code of Practice and Self-Regulation**

Professional bodies develop codes of practice and self-regulation to maintain high standards of professionalism. The Singapore Medical Council, a quasi-judicial body governed by the Medical Registration Act, has jurisdiction in professional misconduct which includes unauthorised disclosure of medical information.<sup>18</sup> The Ministry of Health Guideline for Good Clinical Practice is an adaptation of the International Conference on Harmonisation Tripartite Guideline E6: Note for Guidance on Good Clinical Practice.<sup>19</sup> It is aimed at the conduct of clinical trials of drugs and medical products. The guideline outlines the informed consent to be obtained from the trial subject, including direct access by officials of the Ministry of Health, members of the Ethical Committee or Medical Clinical Research Committee to the patient's original medical record for verification of clinical trial procedure and data. The investigator should ensure the accuracy, completeness, legibility, and timeliness of the data. He should also take measures to prevent accidental or premature destruction of these documents.

### **COMPARISON OF PRIVACY PROTECTION IN SINGAPORE WITH THE EUROPEAN COMMUNITY DIRECTIVE ON DATA PRIVACY 1995**

Data and information privacy in Singapore is assured by the courts through common law and some specialty-related statutes. These provisions ensure confidentiality of information. For data captured electronically on computer, the Computer Misuse Act provides good security of the data from unauthorised modification of contents and access to the data. No such assurance is available for paper records of data. The quality of data as set out by the EU Directive is not protected legally in Singapore, although the code of practice from the Guideline for Good Clinical Practice has recommended appropriate measures to be taken to ascertain accuracy, timeliness and protection from destruction. Some statutes stipulate a requirement for informed consent for certain medical information collection but most clinical data collection in large registries are performed without patients' consent. However, the stark contrast between the EU and Singapore in personal data protection is the lack of the patient's right to access to the collected data or right to object processing of data related to him or her in Singapore (Appendix 1). Evidently, by the

standard set by the EU Directive, Singapore has a long way to go in protecting privacy in medicine.

The EU Directive has a potentially profound impact on the growth of Singapore's economy and on medical and life science research. Indeed, more than 30 countries worldwide have enacted data protection legislation along the EU Directive to avoid potential economic loss when the member states of the EU strictly enforce privacy laws on data protection, in particular when transborder transfer of data to a destined country without adequate protection of data privacy is prohibited.

One of the new economic strategies recently identified is the development of Singapore into a regional hub for the healthcare industry and life science research. Transborder movement of patients, patient-related data and research data will necessarily increase. A lack of privacy law on medical data to an adequate level as stipulated by the EU Directive may be an obstacle for Singapore compared to other regional countries, such as Australia where the amended Privacy Act 1988 with a section on health services came into action on 21 December 2001.

The public's desire for confidentiality in medical data is evidently well protected. However, the extent of privacy in data processing leaves much to be desired in Singapore. The lack of public debate may indicate a low domestic demand for legislation of a privacy law. Nonetheless, legislators may find the external demands and economic competition strong forces for such a legislature in Singapore.

## CONCLUSION

The EU Directive provides a legal framework for good clinical practice which protects patients' privacy in confidentiality and unauthorised disclosure of the patients' identity. The legality, purpose and quality of data are assured with patients' informed consent. Patients are given the right to access to the data and right to object processing of data when there is a legitimate and appropriate justification.

Strict application of these directives imposes some practical difficulties, especially in obtaining adequate informed consent in data collection and in secondary processing of the data for medical research. A fine balance between protection of sensitive data and practicality must be achieved.

Singapore does not have a privacy law. Patients' confidentiality is protected by common law. Computerised records are protected from unauthorised access to the data, disclosure of data and modification

of contents by the Computer Misuse Act. The level of privacy protection is far below the stipulations in the EU Directive. Transfer of data to and from Singapore to third countries maybe prohibited by countries imposing data privacy protection. Data privacy protection is an important initiation to keep Singapore abreast and competitive with other countries.

## REFERENCES

1. Privacy Protection Study Commission. Personal privacy in an information society. Washington DC, 1977.
2. Mandl KD, Szolovits P, Kohane IS. Public standards and patients' control: how to keep electronic medical records accessible but private. *BMJ* 2001; 322:283-7.
3. Sands DZ. Electronic patient-centered communication: managing risks, managing opportunities, managing care. *Am J Manag Care* 1999; 5:1567-71.
4. Computer Science and Telecommunications Board, National Research Council. For the record: protecting electronic health information. Washington DC: National Academy Press, 1997.
5. European Community Directive on Data Privacy 1995. *Official Journal of the European Communities* 1995; L281:31.
6. Berry RM. The genetic revolution and the physician's duty of confidentiality. The role of the old Hippocratic virtues in the regulation of the new genetic intimacy. *J Leg Med* 1997; 18:401-41.
7. Woodward B. The computer-based patient record and confidentiality. *N Eng J Med* 1995; 333:1419-22.
8. Health Privacy Working Group. Best principles for health privacy. A report of the Health Privacy Working Group, Institute for Health Care Research and Policy. Washington DC: Georgetown University, 1999.
9. Health Privacy Polling Data. Health Privacy Project, Institute of Health Care Research and Privacy. Washington DC: Georgetown University, 1999.
10. Ciment J. US Congress considers medical privacy bill. *BMJ* 1999; 318:962.
11. Mandl KD, Kohane IS, Brandt AM. Electronic patient-physician communication: problems and promises. *Ann Int Med* 1998; 129:495-500.
12. Bakker A. Security in perspective, luxury or must? *Int J Med Inf* 1998; 49:31-7.
13. Epstein MA, Pasioka MS, Lord MP, Wong ST, Mankovich NJ. Security for the digital information age of medicine: issues, application and implementation. *J Digit Imaging* 1998; 11:33-44.
14. Rind DM, Kohane IS, Szolovits P, Safran C, Chueh HC, Bennett GO. Maintaining the confidentiality of medical records shared over the internet and the world wide web. *Ann Int Med* 1997; 127:138-41.
15. Reardon J, Rogers R. Recommendations for International Action. Barriers to a Global Information Society for Health. Report from the Project G8-Enable. Amsterdam: IOS Press, 1999.
16. Organisation for Economic Cooperation and Development Committee for Scientific and Technology Policy. Data protection in transborder flows of health research data, 1999.
17. *Coco v A.N. Clarke (Engineers) Ltd. [1969] RPC 41 (Ch.)*.
18. The SMC Ethics Code. Singapore Medical Council, 1995.
19. Singapore Guidelines for Good Clinical Practice. Ministry of Health, Singapore, 1999.

APPENDIX 1

Comparison of data privacy in medicine between EU and Singapore.

| Privacy Attributes  | EU | Singapore |      |      |
|---|----|-----------|------|------|
|   |    | CL        | Stat | Code |
| Category of Data  |    |           |      |      |
| 1. Race/Ethnic  | +  | -         | -    | -    |
| 2. Political Opinion  | +  | -         | -    | -    |
| 3. Religion/Philosophy  | +  | -         | -    | -    |
| 4. Trade union membership   | +  | -         | -    | -    |
| 5. Health/sex history   | +  | -         | -    | -    |
| Quality of Data   |    |           |      |      |
| 1. Obtained and processed legally/lawfully                          | +  | +         | +    | +    |
| 2. Held for specific, explicit & legitimate purposes                | +  | +/-       | -    | -    |
| 3. Adequate, complete, up to date                                   | +  | -         | -    | +/-  |
| 4. Held no longer than necessary                                    | +  | +/-       | -    | +/-  |
| Informed Consent  | +  | +         | +    | +    |
| Right to Access to Data   |    |           |      |      |
| 1. Confirm data has been collected                                  | +  | -         | -    | -    |
| 2. Purpose of processing  | +  | -         | -    | -    |
| 3. Category of data collected                                       | +  | -         | -    | -    |
| 4. Recipient or category of recipient to whom the data are destined | +  | -         | -    | -    |
| Right to object processing of data                                  | +  | -         | -    | +/-  |
| Confidentiality   | +  | +         | +    | +    |
| Security  | +  | +/-       | +/-  | +/-  |

Note: “+”=definite feature; “-”=clearly absent; “+/-”=unclear, “CL”=Common Law; “Stat”=Statutes; “Code”=Code of Practice.