IS YOUR MEDICAL INFORMATION SAFE? A COMPARISION OF COMPREHENSIVE AND SECTORAL PRIVACY AND SECURITY LAWS

Rebecca L. Woodard[1]

I. INTRODUCTION

The privacy of an individual's personal information has long been considered sacred.[2] The use of electronic data and communication has rapidly changed the way the world communicates.[3] Globalization,[4] convergence,[5] and multi-media[6] have all impacted the security of data and information.[7] There has been an increase in the weight placed on security of data because of the changes in the way data is stored and transferred.[8] When information is stored and/or transferred electronically, there is increased potential for the information to be misused or mishandled, leading to an infringement of individual privacy.[9]

This Note will look at why personal information, and specifically personal health information, should be protected and how governments around

---

1. J.D., Indiana University School of Law – Indianapolis, 2005 *(expected);* B.S., Physical Therapy, Northeastern University, Boston, Massachusetts, 2000.

2. *See generally* RESTATEMENT (SECOND) OF TORTS: INVASION OF PRIVACY § 652B (1977); *see also* David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments,* 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 3 (Fall 1999).

3. *See* John Graubert & Jill Coleman, *The Impact of Technological Change in the Canada/U.S. Context: Consumer Protection and Antitrust Enforcement at the Speed of Light: The FTC Meets the Internet,* 25 CAN.-U.S. L.J. 275, 275 (1999).

4. Banisar *supra* note 2, at 5. "GLOBALIZATION removes geographical limitations to the flow of data. The development of the Internet is perhaps the best known example of a global technology." *Id.*

5. *Id.* "CONVERGENCE is leading to the elimination of technological barriers between systems. Modern information systems are increasing inter-operable with other systems, and can mutually exchange and process different forms of data." *Id.*

6. *Id.* "MULTI-MEDIA fuses many forms of transmission and expression of data and images so that information gathered in a certain form can be easily translated into other forms." *Id.*

7. *Id.* at 4-5.

8. *See* William J. Kambas, *A Safety Net in the E-Marketplace: The Safe Harbor Principles Offer Comprehensive Privacy Protection Without Stopping Data Flow,* 9 ILSA J. INT'L & COMP. L. 149, 168 (2002).

9. *See id.*

> Collection of consumer data will inevitably yield files of consumer data. Once these files are created, they must be protected from misuse (both internal and external) and from inadvertent dissemination. Measures must be taken to ensure the security of information collected. That which is not secure cannot be considered private.

Id.

the world are addressing current and potential security problems. Part II looks at a brief history of the privacy and security of personal health information and how it has evolved with the integration of technology. Part III focuses on how personal information can be misused and why it is so important to maintain the security of personal health information. Part IV addresses the history of privacy laws in the United States, Canada, and the United Kingdom. Part V is dedicated to current and future privacy and security laws. Part VI looks at the issues of compliance and penalties for violations of the regulations. Lastly, Part VII looks at the strengths and weaknesses of the different methods of regulation..

II. THE CHANGES IN THE PRIVACY AND SECURITY OF PERSONAL INFORMATION

There have been many changes in the way societies view privacy since the days when Warren and Brandeis described privacy as the "right to be left alone."[10] In 1948, the Universal Declaration of Human Rights stated that "[n]o one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour [sic] or reputation. Everyone has the right to the protection of the law against such interferences or attacks."[11] The concept of keeping medical information private has existed since at least 400 B.C. when Hippocrates wrote the Hippocratic Oath.[12] "Whatever, in connection with my professional practice or not, in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret."[13] Through time, the Oath has changed; nevertheless, the emphasis on privacy of health information remains strong.[14]

With the growth of electronic technology, the methods of collecting, storing, and transferring data have changed in two major ways.[15] Prior to the

10. *See* Banisar, *supra* note 2, at 8 (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 193, 193 (1890)).

11. *Id.* at 8 (quoting Human Rights Web, U.N. Universal Declaration of Human Rights, at http://www.hrweb.org/legal/udhr.html (July 6, 1994) (ed. Jan. 27, 1997)).

12. *See* Hippocrates, *The Oath,* The Internet Classics Archive, Francis Adams trans., http://classics.mit.edu/Hippocrates/hippooath.html (n.d.) (last visited September 7, 2004).

13. *Id.*

14. *See* Louis Lasagna, *The Hippocratic Oath – Modern Version, Nova Online, at* http://www.pbs.org/wgbh/nova/doctors/oath_modern.html (n.d.) (last visited Oct. 30, 2004). "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know." *Id.* The Modern Oath was "[w]ritten in 1964 by Louis Lasagna, Academic Dean of the School of Medicine at Tufts University, and used in many medical schools today." *Id.*

15. *See* WILLIAM STALLINGS, NETWORK SECURITY ESSENTIALS, APPLICATIONS AND STANDARDS 2 (2d ed. 2003).

use of computer technology, data was secured physically and administratively.[16] Technology has led to the need for new security components.[17] First, there is the new "need for automated tools for protecting files and other information stored on the computer."[18] Computer security is "[t]he generic name for the collection of tools designed to protect data and to thwart hackers."[19]

The second change is the need for securing the systems that carry the data.[20] "Network security measures are needed to protect data during their transmission."[21] Essentially, all organizations "interconnect their data processing equipment with a collection of interconnected networks. Such a collection is often referred to as an internet, and the term internet security is used."[22] The need for computer security and network security cannot be clearly distinguished, and both must be addressed to ensure data remains private.[23]

There are two types of network security attacks, passive and active.[24] Passive attacks obtain information from the system but do not disrupt the system.[25] Active attacks, on the other hand, do modify the data.[26] Passive attacks can be further divided into two types, the "release of message contents" and "traffic analysis."[27] Both types of passive attacks are harder to detect than active attacks because they do not affect the data, and the transmission appears to have been normal.[28] Although active attacks may be easier to detect, they are more difficult to prevent.[29]

---

16. *Id.* "An example of the former is the use of rugged filing cabinets with a combination lock and for storing sensitive documents. An example of the latter is personnel screening procedures used during the hiring process." *Id.*

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.*

22. *Id.*

23. *See id.*

24. *Id.* at 5.

25. *See id.* "Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information being transmitted." *Id.*

26. *Id.* at 7. "Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service." *Id.*

27. *Id.* at 5.

> The **release of message contents** is easily understood . . . . A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
>
> A second type of passive attack, **traffic analysis** is subtler . . . . Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.

Id.

28. *Id.* at 6.

29. *Id.* at 9.

The growing use of computers has significantly increased the preexisting problems with ensuring the privacy and security of health data.[30] "Health information is perhaps the most intimate, personal, and sensitive of any information maintained about an individual. As the nation's health care system grows in size, scope, and integration, the susceptibility of that information to disclosure will also increase."[31] The major dilemma in the health care field is how to balance the individual's rights to the privacy of his or her medical records with the use of a system that improves communication, decreases costs, and improves quality of care.[32] Without a certain expectation of privacy, patients will be unwilling to disclose critical information that may be detrimental to their health care.[33]

III. HOW YOUR INFORMATION CAN BE MISUSED

Currently, there are three general types of misuses of health data with the use of electronic data storage and transmission: "individuals who misuse medical data," "use of personal health data for marketing," and "institutional practices that do cause unambiguous harm to identifiable individuals."[34] There are numerous examples of cases of individual misuse of personal data.[35] For example, "Arthur Ashe's positive HIV status was disclosed by a health care

---

30. *See* Paul Starr, *Health and the Right to Privacy*, 25 AM. J.L. & MED. 193, 196 (1999).

31. Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 454 (1995).

32. *See* Mark Weitz et al., *In Whose Interest? Current Issues in Communicating Personal Health Information: A Canadian Perspective*, 31 J.L. MED. & ETHICS 292 (2003).

33. Irwin Kleinman, MD et al., *Bioethics for Clinicians: 8. Confidentiality*, 156 CANADIAN MED. ASSOC. J. 521, 522 (Feb. 15, 1997), http://www.utoronto.ca/jcb/about/publications/521.pdf (last visited Oct. 11, 2004). The following is a Canadian perspective on "why confidentiality is important:"

> Without an understanding that their disclosures will be kept secret, patients may withhold personal information. This can hinder physicians in their efforts to provide effective interventions or to pursue certain public health goals. For example, some patients may not feel secure in confiding a drug or alcohol dependence and thus may not have the benefit of treatment. Others may refrain from disclosing information that could alert the physician to the potential for harm or violence to others.
>
> Respect for the confidentiality of patient information is not based solely on therapeutic considerations or social utility, however. Of equal, if not greater, importance is the physician's duty to respect patient autonomy in medical decision-making. Competent patients have the right to control the use of information pertaining to themselves. They have the right to determine the time and manner in which sensitive information is revealed to family members, friends and others.

Id.

34. Starr, *supra* note 30, at 197-98.

35. *See id; see also* Health Privacy Project, Medical Privacy Stories, *at* http://www.healthprivacy.org/usr_doc/Privacy_storiesupd.pdf (last updated Nov. 10, 2003) [hereinafter Health Privacy Project].

worker and published by the media without his permission,"[36] and a New York Congresswoman's history of depression was revealed, during a primary election, in a fax from the hospital to the local media.[37] There was also a misuse of data when the identities of 4,000 HIV positive individuals were exposed by a public health worker who sent a disk with the names to the newspaper.[38] All of these examples of data misuse represent an individual's ability to take advantage of the personal data to which they have access.[39]

The second type of misuse of data is "the use of personal health data for marketing and other purposes where the harm to the individual is ambiguous or relatively small."[40] For example, there have been privacy violations when pharmacists have admitted disclosing the list of customers for marketing purposes.[41]

The third general type of misuse of data is the "institutional practices that do cause unambiguous harm to identifiable individuals." This occurs when businesses or organizations get their hands on individual data to discriminate in the way they operate.[42] There are financial incentives to keeping personal health information private.[43] Employers have used health information to discriminate against employees when it is available.[44] Additionally, health information has been used to discriminate against individuals in the business setting.[45]

Today, there are many reasons for keeping personal health information private.[46] Generally, the public fears embarrassment or harm to their reputation when personal heath information becomes known.[47] In 1977, the United States Supreme Court acknowledged the "individual interest in avoiding disclosure of personal matters," in *Whalen v. Roe*.[48] Nevertheless, the court held that a New

---

36. Starr, *supra* note 30, at 197.

37. *Id.*

38. *Id.*

39. *See id.*

40. *Id.* See also Health Privacy Project, *supra* note 35, for additional examples of the misuse of data for marketing.

41. Starr, *supra* note 30, at 197.

42. *See id.* at 198.

43. *See id. See also* Health Privacy Project, *supra* note 35.

44. Charity Scott, *Is Too Much Privacy Bad for Your Health? An Introduction to the Laws, Ethics, and HIPAA Rule on Medical Privacy*, 17 GA. ST. U. L. REV. 481, 486 (2000). Survey of "Fortune 500 employers admitted using their employees' medical records in making employment decisions." *Id.* at 487.

45. *Id.* at 487. For example, "[i]n one well-known account, a banker allegedly was able to use computerized medical records to determine which of his customers had cancer, and he called their loans early." *Id.*

46. *See generally id. See also infra* Part II.

47. *Id.*

48. 429 U.S. 589, 599-600 (1977). In the opinion Professor Kurland was quoted saying:

> The concept of a constitutional right of privacy still remains largely undefined. There are at least three facets that have been partially revealed, but their form and shape remain to be fully ascertained. The first is the right of the individual to be

York statute, which recorded the identity of all individuals who received prescriptions for certain classes of drugs in a state database, was not in violation of the Constitution.[49]

Not only has the collection and storage of information changed, but it has become a part of everyday business and is "completely legal."[50] Internet provider companies collect data on their users for advertisers.[51] Health information is also becoming big business.[52]

> As health care has been transformed into a complex industry representing one-seventh of the economy, organizations of all kinds—employers, insurers, plans, networks, systems, pharmaceutical makers, device makers and many others—have had growing interests in data to control their costs, increase their revenues or improve their performance in some other dimension. They have been willing to invest in information, to pay for information, to sell information—information itself has become a business.[53]

Despite the business incentives to use and collect health information, there are strong incentives to protect the information.[54] According to Gostin, there are two independent reasons for protecting health information.[55] The first reason is simple: "the personal nature of health data."[56] The second reason is more complex.[57] The rapid transition to electronic records has the potential to lead to increased harm to the patient, to the providers, and to the patient-provider relationship due to the vast amount of data that can be stored on individuals.[58] Both reasons are significant incentives to find solutions for current potential problems of medical records disclosure.[59]

> free in his private affairs from governmental surveillance and intrusion. The second is the right of an individual not to have his private affairs made public by the government. The third is the right of an individual to be free in action, thought, experience, and belief from governmental compulsion.

Id. at 599 n.24.

49. *Id.* at 603-04.

50. *See* Jessica Litman, *Cyberspace and Privacy: A New Legal Paradigm? Information Privacy/Information Property,* 52 STAN. L. REV. 1283, 1284 (2000).

51. *Id.*

52. Starr, *supra* note 30, at 196.

53. *Id.*

54. *See* Lawrence O. Gostin etal, *The Nationalization of Health Information Privacy Protections,* 8 CONN. INS. L.J. 283, 284-85 (2001-02) [hereinafter *Nationalization of Health Information Privacy Protections*].

55. *Id. at 284.*

56. *Id.*

57. *See id. at 284-85.*

58. *See id.* Gostin describes the second reason as:

> [T]he rapid shift from paper to electronic records. Health information used by health providers, insurers, and data processors can include intimate details about the patient's mental and physical health as well as information about their social behaviors, personal relationships, and financial status. Unwarranted disclosures

At this point, Canada, the United States, Europe, New Zealand, and Australia have all passed or are in the process of passing legislation that will affect how health information can be used.[60] Each government has acknowledged the need for regulation in this area; nevertheless, there is little standardization in their approaches.[61] This Note will look at the progress of privacy rights of patients in the United States, Canada, and the United Kingdom. It will focus on the current and forthcoming legislation that is available to protect an individual's personal health information. It will also look at what security provisions are in place to protect the data, as well as the penalties for violations. This Note will also compare how each government views personal information and how that affects policy-making. Lastly, it is the goal of this Note is to determine whether one system is more successful than the others and to identify changes that should be made.

IV. THE HISTORY OF PRIVACY OF HEALTH INFORMATION

There are different models of privacy protections that governments can employ, with some approaches used in combination.[62] The four major methods of protection are comprehensive laws, sectoral laws, self-regulation, and technologies of privacy.[63] The United States, Canada, and Europe all have a history of legislative action that focuses on the protection of information and individual privacy.[64]

Comprehensive laws are used by creating a general law that "governs the collection, use and dissemination of personal information by both the public and private sectors."[65] This is the method used by the European Union, and a variation of this method is also being used in Canada.[66] The system used in Canada is a "co-regulatory model," which has the industry developing the standards and implementing them, while the standards are overseen by the governmental privacy agency.[67]

Sectoral laws are created through separate legislation for each industry, rather than having a general data protection law.[68] This is a more complicated system because it requires more legislation and "protections frequently lag

---

of this information could lead to societal stigmatization and discrimination by employers, insurers, and others, as well as a loss of patient trust in medical providers.

Id.

59. *See id.*

60. Weitz et al., *supra* note 32.

61. *See id.*

62. *See* Banisar, *supra* note 2, at 13-14.

63. *Id.*

64. *See id.* at 14-15. For a more detailed explanation of the legislative history of data protection see *id.* at 10-13.

65. *Id.* at 13.

66. *Id.* at 13-14.

67. *Id.*

68. *See id.*

behind" the technology.[69] The United States uses this type of system, and "[t]he lack of legal protections for medical and genetic information in the U.S. is a striking example of the limitations of these laws."[70] Nevertheless, sectoral laws can be a positive supplement to comprehensive legislation.[71]

Self-regulation places the burden on the industry or entity to "establish codes of practice."[72] The model of self-regulation makes it difficult to ensure enforcement, and the codes have a propensity to be weak.[73] However, as of 1999, self-regulation was the "policy promoted by the governments of the U.S., Japan, and Singapore."[74]

Lastly, privacy can be regulated by the use of privacy technology.[75] Technology-based systems give the user privacy protections by using different technologies including: "encryption, anonymous remailers, proxy servers, digital cash and smart cards.[76] Questions remain about security and trustworthiness of these systems. Recently, the European Commission evaluated some of the technologies and stated that the technological tools would not replace a legal framework, but could be used to compliment the existing laws."[77]

A. The United States

The United States does not have comprehensive privacy laws that pertain to all types of private industries.[78] In addition, the United States lacks a single agency that oversees privacy,[79] Instead, the United States uses industry specific rules.[80] For example, there are consumer protection laws for personal information contained in bank, credit card, other financial records, and even video rentals.[81] In 1996, the U.S. Congress enacted The Health Insurance Portability and Accountability Act of 1996 (HIPAA).[82] HIPAA provides

---

69. *Id.*

70. *Id.* This article was written in 1999, prior to the current HIPAA regulations. However, the new laws continue to be sectoral in nature. *See* Health Insurance Portability & Accountability Act of 1996, *infra* note 82.

71. *Banisar, supra* note 2, at 13-14.

72. *Id. at* 14.

73. *Id.*

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.*

78. *Id.* at 108.

79. *Id.* at 109. "The Federal Trade Commission (FTC) has oversight and enforcement powers for laws protecting consumer credit information and fair trading practices, but has no authority to enforce privacy rights, other than those arising from fraudulent or deceptive trade practices." *Id.* at 109.

80. *See id.*

81. *Id.*

82. *See* Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104-191 (1996) (codified at 45 C.F.R. pts. 160, 162 & 164).

mandates for the Department of Health and Human Services to adopt standards for the security of electronic health information,[83] draft mandates for providers to comply, and to recommend privacy regulations to Congress within twelve months.[84] If nothing has been accomplished by Congress, then the Department of Health and Human Services may create regulations[85] for the bill, pre-empt state law,[86] and provide civil penalties for violations.[87]

HIPAA was developed by the U.S. Department of Health and Human Services and has come into effect in stages, including the Privacy Rule in 2003[88] and the Security Rule,[89] which was finalized in February 2003, but does not require full compliance until April 21, 2005.[90] The Privacy Rule generally covers any "individually identifiable health information."[91]

The HIPAA Security Rule was developed because, until this point, "no standard measures exist[ed] in the health care industry that address[ed] all aspects of the security of electronic health information while it [was] being stored or during the exchange of that information between entities."[92] "The purpose of this final rule is to adopt national standards for safeguards to protect

---

To amend the Internal Revenue Code of 1986 to improve portability and continuity of health coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Id.

83. *Id.* § 1173. This section states that:

(1) IN GENERAL. The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically that are appropriate for --

(A) the financial and administrative transactions described in paragraph (2); and

(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

Id. See *id.* § 1173(a)(2) for a list of transactions referred to in paragraph (1).

84. *See id.* § 1174.

85. *See id.* § 1175.

86. *See id.* § 1178.

87. *See id.* § 1176.

88. *See* Standards for Privacy of Individually Identifiable Health Information; Final Rule, 67 Fed. Reg. 53,182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160, 162 & 164).

89. *See* Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164).

90. *Id.*

91. *See* Dept. of Health and Human Services, Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule, NIH Publ. num. 03-5388, p. 2 (2002), http://www.privacyruleandresearch.nih.gov/pr_02.asp (last revised Sept. 25, 2003)

The Privacy Rule establishes minimum Federal Standards for protecting the privacy of individually identifiable health information. The Rule confers certain rights on individuals, including rights to access and amend their health information and to obtain a record of when and why their PHI [personal health information] has been shared with others for certain purposes.

Id.

92. Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. at 8,334.

the confidentiality, integrity, and availability of electronic protected health information."[93] The Security Rule applies when the data is in the custody of the covered entities and during transmission of the data.[94]

B. Canada

The Canadian method of protecting data is different than the new HIPAA[95] rules in the United States in that it does not apply exclusively to health information.[96] In 2000, Canada enacted the Personal Information Protection and Electronic Documents Act (Canadian Act).[97] The purpose of the act is:

> to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act[.][98]

The Act is broken into five parts.[99] "Part 1 of this enactment establishes a right to the protection of personal information collected, used or disclosed in the course of commercial activities . . . ."[100] This includes all private and governmental operations both within Canada and internationally.[101] Additionally, it provides that the Privacy Commissioner will be responsible for taking complaints.[102] Part 2 of the Canadian Act looks at using electronic data storage where regulations provide for the use of paper records as well as for the

---

93. *Id.*

94. *Id.*

95. *See generally* Health Insurance Portability & Accountability Act of 1996.

96. Personal Information Protection and Electronic Documents Act, R.S.C., ch. 5 (2000) (Can.), http://www.privcom.gc.ca/legislation/02_06_01_e.agp (last visited Oct. 19, 2003).

97. *Id.*

98. *Id.*

99. *Id.* at Summary.

100. *Id.*

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

Id. at 4, pt. 1, § 3.

101. *See id.*

102. *See id.* at 25, pt. 2. "The purpose of this Part is to provide for the use of electronic alternatives in the manner provided for in this Part where federal laws contemplate the use of paper record or communicate information or transactions." *Id.*

use of electronic signatures.[103] Part 3 of the Canadian Act "amends the *Canadian Evidence Act* to facilitate the admissibility of electronic documents" and provides for how they can be used.[104] Parts 4 and 5 address the publication of documents electronically.[105] Parts 1 and 2 are the most relevant to the protection of health information and its security because Part 1 defines what information is considered "personal health information,"[106] and Part 2 looks at the computer security aspects of the information and the regulation thereof.[107]

C. *The United Kingdom*

In 1998, the United Kingdom enacted the Data Protection Act 1998.[108] The Data Protection Act generally includes an explanation of the rights of data subjects,[109] the role of the data controllers,[110] those exempted from the Act,[111] and enforcement of the Act.[112] The exemptions provided for in The Data Protection Act are extensive; they include exemptions for national security, crime and taxation, health, education, social work, regulatory activity, and more.[113] The Freedom of Information Act 2000 (FOIA)[114] was enacted in order to create a "[g]eneral right of access to information held by public authorities."[115] FOIA is intended to "amend the Data Protection Act of 1998 and the Public Records Act of 1958."[116] It broadened the rights created in the Data Protection Act.[117] "[FOIA] creates a statutory right of access, provides for

---

103. *Id.* at Summary.

104. *Id.*

105. *Id.*

106. *See id.* at 3, pt. 1.

107. *See id.* at 29, pt. 2.

108. *See* Data Protection Act, 1998, c. 29 (Eng.), http://www.hmso.gov.uk/acts/acts1998/19980029.htm (last visited Oct.11, 2004). The purpose of the Act is to create "[a]n act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information." *Id.*

109. *See id.* at pt. II, § 7.

110. *Id.* at pt. I, § 1(1). Data controller means "a person who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed." *Id.*

111. *Id.* at pt. IV.

112. *See generally id.*

113. *See generally id.* at pt. IV.

114. Freedom of Information Act, 2000, c. 36 (Eng.) (2000), http://www.legislation.hmso.gov.uk/acts/acts2000/20000036.htm (last visited Sept 7, 2004).

115. *Id.*

116. *Id.* An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act of 1998 and the Public Records Act of 1958; and for connected purposes. *Id.*

117. *See id.* at pt. I, § 1. "(1) Any person making a request for information to a public authority is entitled[:] (a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and (b) if that is the case, to have that information communicated to him." *Id.* See the Data Protection Act, 1998, c. 29 (Eng.) for the rights originally conferred in the Data Protection Act.

a more extensive scheme for making information publicly available, and covers a much wider range of public authorities including: local government, National Health Service bodies, schools and colleges, the police, and other public bodies and offices."[118]

The Data Protection Act and FOIA are both in compliance with the 1995 European Union Directive 95/46/EC (Directive 95/46/EC)[119] on the protection of individuals with regard to the processing of data and on the free movement of such data.[120] The general objective of the Directive 95/46/EC is to ensure that the member states:

> [P]rotect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Member states shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph [one]."[121]

The Directive sets up a structure to define what data is protected, who is responsible for the protection of data, and guidelines on how it is to be protected.[122]

More recently, the European Union put out Directive 2002/58/EC of the European Parliament, and of the Council of July 12, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector.[123] The member states of the European Union are required to comply with the directives, and as of January 2000, the European Union had taken action against five member states for non-compliance.[124]

V. PRIVACY AND SECURITY RULES

A. United States

The Privacy Rule created under HIPAA was developed to increase consumer confidence in privacy by requiring that the entities involved in heath

---

118. Explanatory Notes to Freedom of Information Act, 2000, c. 36 (Eng.), http://www.hmso.gov.uk/acts/en2000/2000en36.htm (last visited Oct. 19, 2003).

119. Council Directive 95/46/EC, 1995 O.J. (L 281) 31. Article 4 National Law Applicable, states that: "[e]ach Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data . . . ." *Id.* at ch. I, art. 4.

120. *See id.*

121. *Id.* at ch. I, art. 1.

122. *See generally id.*

123. Council Directive 2002/58/EC, 2002 O.J. (L 201) 37.

124. *Data Protection: Commission Takes Five Member States to Court,* Press Release Rapid, Brussels (Jan. 11, 2000), http://www.europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/00/10/AGED7dg=EN&display= (last visited Oct. 19, 2003) (on file with author).

care "guard against misuse" of information and "limit the sharing of such information."[125] Further, it gives consumers new rights to access and control the information.[126] The United States defines exactly what information is covered by HIPAA in the Privacy Rule.[127] The rule covers three types of organizations: health plans, health care clearinghouses, and health care providers who conduct business electronically.[128] Health plans are given a broad definition and provide exclusions for some limited government programs.[129] Heath care clearinghouses are the organizations that process

125. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,182.

126. *See id.*

127. *See* Dep't of Health and Human Services Administrative Services and Related Requirements, 45 C.F.R. § 160.103 (1999). This section provides an extensive list of definitions. *See id.*

128. 45 C.F.R. § 160.102 (2002).

129. *See* 45 C.F.R. § 160.103 (2002), which provides:

> Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)). (1) Health plan includes the following, singly or in combination: (i) A group health plan, as defined in this section. (ii) A health insurance issuer, as defined in this section. (iii) An HMO, as defined in this section. (iv) Part A or Part B of the Medicare program under title XVIII of the Act. (v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq. (vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)). (vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy. (viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers. (ix) The health care program for active military personnel under title 10 of the United States Code. (x) The veterans health care program under 38 U.S.C. chapter 17. (xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)). (xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq. (xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq. (xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq. (xv) The Medicare+Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28. (xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals. (xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)). (2) Health plan excludes: (i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and (ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition): (A) Whose principal purpose is other than providing, or paying the cost of, health care; or (B) Whose principal activity is: (1) The direct provision of health care to persons; or (2) The making of grants to fund the direct provision of health care to persons.

health information in some manner.[130] Health care providers include all medical and healthcare professionals that bill for services.[131]

The code also explicitly describes what information is protected.[132] "Protected health information means individually identifiable health information . . . ."[133] This includes information that is transmitted or maintained by electronic media or any other means.[134] Protected health information does not include some individually identifiable health information that is defined in some specific education and employment records, as identified by statute.[135] "Transaction means the transmission of information between two parties to carry out financial or administrative activities related to healthcare."[136] This includes:

> (1) Health care claims or equivalent encounter information. (2) Health care payment and remittance advice. (3) Coordination of benefits. (4) Health care claim status. (5) Enrollment and disenrollment in a health plan. (6) Eligibility

---

130. *Id.*

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Id.

131. *See id.*

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Id.

132. *See id.*

133. *Id.*

134. *Id.*

135. *Id.*

(2) Protected health information excludes individually identifiable health information in: (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity in its role as employer.

Id.

136. *Id.*

> for a health plan. (7) Health plan premium payments. (8) Referral certification and authorization. (9) First report of injury. (10) Health claims attachments. (11) Other transactions that the Secretary may prescribe by regulation.[137]

The Code of Federal Regulations sets out the Administrative Requirements in Part 162.[138] Part of the purpose of the new rules is to improve the Administrative Simplicity.[139] Code sets are used make the data manageable.[140] There are medical data code sets and nonmedical data code sets that the covered entities must use.[141] Medical data code sets are used "at the time the health care is furnished,"[142] and nonmedical code sets are used "at the time the transaction is initiated."[143]

Part 164 of the Code of Federal Regulations defines the "security standards for the protection of electronic protected health information."[144] Generally, there are four things that the covered entities must do.[145] First, covered entities must "[e]nsure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits."[146] Second, they must "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information."[147] Third, they must "[p]rotect against any reasonably anticipated uses or disclosures of such information that are not permitted or required . . . ."[148] Lastly, the covered entity must "[e]nsure compliance . . . by its workforce."[149]

There is some flexibility given to the covered entities in how they comply with the four general requirements as long as they can put into practice the

---

137. *Id.*

138. *See generally* 45 C.F.R. § 162 (2003).

139. *See* Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53,182.

> [S]ections 261-264 of the statute were designed to improve the efficiency and effectiveness of the health care system by facilitating the electronic exchange of information with respect to certain financial and administrative transactions carried out by health plans, health care clearinghouses, and health care providers who transmit information electronically in connection with such transactions.

Id.

140. *See* 45 C.F.R. § 162.103. "Code set means any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. A code set includes the codes and the description of the codes." *Id.* For more detailed definitions and examples of the code sets see 45 C.F.R. § 162.1002 (2003).

141. 45 C.F.R. § 162.1000 (2002).

142. *Id.* § 162.1000(a).

143. *Id.* § 162.1000(b).

144. 45 C.F.R. § 164.306 (2003).

145. *Id.* § 164.306(a).

146. *Id.* § 164.306(a)(1).

147. *Id.* § 164.306(a)(2).

148. *Id.* § 164.306(a)(3).

149. *Id.* § 164.306(a)(4).

standards of the Security Rule.[150] This gives the covered entity the flexibility to factor in the size of the organization, their "technical infrastructure, hardware, and software security capabilities," the costs associated with the technology, and the potential for risk to the electronically protected health information.[151] There are some standards for which compliance is mandatory.[152]

There are two types of specifications found in the Security Rule: those that are required and those that are addressable.[153] For the required standards the "covered entity must implement" the standards;[154] however, the requirements are different when the standard is addressable.[155] When a provision is deemed addressable, the covered entity must: "[a]ssess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information."[156] Following the assessment, the entity must: "[i]mplement the implementation specification if reasonable and appropriate."[157] If the specification is not appropriate, then the entity must document why it was not appropriate and implement a substitute appropriate measure.[158] Lastly, there must be regular review and modification of the covered entity's protection of electronic health information.[159]

All of the security measures are broken down into three types of safeguards used to protect information: administrative, physical, and technical.[160] Administrative safeguards function by using "policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."[161]

There are eight mandatory administrative standards, which include: devising a security management process,[162] assigned security responsibility,[163] workforce security,[164] information access management,[165] security awareness

150. *See id.* § 164.306(b).
151. *Id.* § 164.306(b)(2).
152. *Id.* § 164.306(c).
153. *Id.* § 164.306(d)(1).
154. *Id.* § 164.306(d)(2).
155. *See id.* § 164.306(d)(3).
156. *Id.* § 164.306(d)(3)(i).
157. *Id.* § 164.306(d)(3)(A).
158. *Id.* § 164.306(d)(3)(B).
159. *Id.* § 164.306(e).
160. 45 C.F.R. § 164.304.
161. *Id.*
162. 45 C.F.R. § 164.308(a)(1) (2003). The process must include specifications for risk analysis, risk management, a sanction policy and an information system activity review. *Id.*
163. *Id.* § 164.308(a)(2). This provision ensures that there is an identified person responsible for compliance with the security provisions. *Id.*
164. *Id.* § 164.308(a)(3). This section requires that covered entities have the appropriate access to information and that individuals that do not have access cannot get unauthorized access. *Id.* However, the specifications of this provision are addressable rather than required.

and training,[166] security incident procedures,[167] contingency plan,[168] and finally, the covered entity must provide for periodic evaluation of the system.[169] In addition to the required provisions, they may allow "a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances . . . that the business associate will appropriately safeguard the information."[170]

Physical safeguards include "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion."[171] There are four standards for physical safeguards.[172] First, a covered entity must provide facility access controls that prevent unauthorized access to where the information is stored; this includes having contingency operations, a facility security plan, access control and validation procedures, and proper maintenance records.[173] Second, there must be policies and procedures for utilization of a workstation.[174] Third, there must be provisions for workstation security.[175] Finally, there must be policies and procedures that apply to device and media control.[176]

Id. The addressable specification include authorization/supervision, clearance and termination procedures. *Id.*

165. *Id.* § 164.308(a)(4). This provision has a combination of required and addressable provisions. *Id.* If the entity uses a health care clearinghouse, they must confirm that the clearinghouse also complies with the provisions and the addressable provision deals with access to workstations and modification of that access. *Id.* Work station is defined as "an electronic computing device, for example, a laptop or desktop computer, or any device that performs similar functions, and electronic media is stored in an immediate environment." 45 C.F.R. § 164.304.

166. 45 C.F.R. § 164.308(a)(5). This training must apply to the entire workforce, including management. *Id.*

167. *Id.* § 164.308(a)(6). The provision requires there be a response and the reporting of all incidents. *Id.* "Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system." 45 C.F.R. § 164.304.

168. 45 C.F.R. § 164.308(a)(7). This includes having a backup system, disaster recovery plan, emergency operation mode, testing of the plans, and assessment. *Id.*

169. *Id.* § 164.308(a)(8).

170. *Id.* § 164.308(b)(1).

171. 45 C.F.R. § 164.304.

172. 45 C.F.R. § 164.310.

173. *Id.* § 164.310(a).

174. *Id.* § 164.310(b). "Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information." *Id.*

175. *Id.* § 164.310(c). "Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users." *Id.*

176. *Id.* § 164.310(d). "Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored." *Id.*

With regard to security of a workstation, this includes the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.[177] There are five standards for technical safeguards, part of which are required, and part of which are accessible.[178] First, there must be access controls including unique user identification, emergency access procedures, automatic logoff, and encryption and decryption of data.[179] Next, there must be audit controls[180] as well as policies and procedures to protect the integrity of the data.[181] The fourth standard provides for policies and procedures for person or entity authentication for those seeking access to electronic protected health information.[182] The last technical safeguard is transmission security, which includes integrity controls and encryption.[183]

---

177. *See* 45 C.F.R. § 164.304.

178. *See generally* 45 C.F.R. § 164.312 (2003).

179. *Id.* § 164.312(a).

> (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4). (2) Implementation specifications: (i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity. (ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. (iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. (iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

Id.

180. *Id.* § 164.312(b). "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." *Id.*

181. *See id.* § 164.312(c). This is accomplished by having a system that authenticates electronic health information to prevent it from improper alteration or destruction. *See id.*

182. *Id.* § 164.312(d). Authentication is defined as "the corroboration that a person is the one claimed." 45 C.F.R. § 164.304.

183. 45 C.F.R. § 164.312(e), which provides:

> Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. (2) Implementation specifications: (i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. (ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

B. Canada

The Canadian Act is set up to generally protect all personal information that is connected with electronic communication or storage.[184] The act differentiates between personal information and personal health information.[185] Personal information is "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization."[186] The definition of personal health information is defined more specifically.

> "[P]ersonal health information"[,] with respect to an individual, whether living or deceased, means (a) information concerning the physical or mental health of the individual; (b) information concerning any health service provided to the individual; (c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual; (d) information collected in the course of providing health services to the individual; or (e) information that is collected incidentally to the provision of health services to the individual.[187]

The Canadian Act essentially applies to all organizations[188] that use or collect personal information.[189] However, there are a few exceptions.[190] The Act does not apply to government institutions that fall under the Privacy Act,[191] individuals maintaining information for personal use,[192] or an organization using it "for journalistic, artistic or literary purposes."[193] The Act mandates

184. *See* Personal Information Protection and Electronic Documents Act, R.S.C. ch. 5 (2000) (Can.).

185. *See id.* at pt. 1.

186. *Id.* at pt. 1, §2.

187. *Id.*

188. *See id.* The Canadian Act defines "organization" as including "an association, a partnership, a person and a trade union." *Id.*

189. *See id.* at pt. 1.

190. *See id.*

191. *Id.* at pt. 1, § 4(2).

192. *Id.* The act does not apply to people maintaining information for the personal use so long as it is not being used; "any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose the information for any other purpose." *Id.*

193. *Id.* "[A]ny organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose." *Id.*

compliance for all organizations,[194] and allows collection of information for reasonable purposes.[195] The statute also outlines the circumstances when information can be collected "without knowledge or consent."[196]

> [A]n organization may collect personal information without the knowledge or consent of the individual only if (a) the collection of data is clearly in the interest of the individual and consent can not be obtained in a timely way; (b) it is reasonable to expect that the collection with the knowledge or consent of the individual would comprise the availability or the accuracy of the information and the collection is reasonable for the purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; (c) the collection is solely for journalistic, artistic or literary purposes; or (d) the information is publicly available and is specified by the regulations.[197]

Furthermore, there is a provision for the use of data without permission.[198] Information may be used without permission if the organization comes across the information and thinks that it would be helpful for the investigation of previous, current, or future crimes, and the information is used in investigating the crime.[199] Personal information can also be used without consent in situations where there is an emergent threat to life or security,[200] or for academic and research purposes.[201]

There are also provisions for when information can be disclosed without consent.[202] Personal information may be disclosed without consent when it is made to an official or counsel representing the client,[203] for debt collection,[204]

---

194. *Id.* at pt. 1, div. 1. All mandates are indicated with the use of the word "shall" and recommendations are indicated with the word "should." *Id.*

195. *See id.* at pt 1, div. 1. "An organization may collect, use or disclose personal information for purposes that a reasonable person would consider are appropriate in the circumstances." *Id.* at pt. 1, div. 1, § 5(3).

196. *Id.* at pt. 1, div. 1, § 7.

197. *Id.*

198. *Id.* at pt. 1, div. 1, § 7(2).

199. *Id.*

200. *Id.*

201. *Id.* at pt. 1. div. 1, § 7(2)(c). The statute defines the academic exception as when:

> it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used.

Id.

202. *Id.* at pt.1, div. 1, § 7(3).

203. *Id.* Information may be disclosed when "made to, in the Province of Quebec, an advocate or notary, or in any other province, a barrister or solicitor who is representing the organization." *Id.* at pt. 1, div. 1, § 7(3)(a).

when complying with an order of the court,[205] and to a government official that has requested the information for the purpose of national security, law enforcement, and administration of the law.[206] There are additional permitted disclosures for investigation, research, emergency situations, and the conservation of records.[207]

Part 2 of the Canadian Act addresses electronic documents.[208] The Canadian Act defines data as "representations of information or concepts, in any form."[209] It defines an electronic document as "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or computer system or other similar device."[210] "It includes a display, printout or other output of that data."[211]

There are ten principles set forth in Schedule 1 of the Canadian Act: 1) accountability, 2) identifying purposes, 3) consent, 4) limiting collection, 5) limiting use disclosure and retention, 6) accuracy, 7) safeguards, 8) openness, 9) individual access, and 10) challenging compliance.[212] The seventh principle, entitled safeguards, provides that the information will be protected differently depending on the "sensitivity of the information."[213] The rule does not define which information is sensitive.[214]

> The form of consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.[215]

---

204. *Id.* at pt. 1, div. 1, § 7(3)(b).
205. *Id.* at pt. 1, div. 1, § 7(3)(c).
206. *Id.* at pt. 1, div. 1, § 7(3)(d).
207. *Id.* at pt. 1, div. 1, § 7(3).
208. *See id.* at pt. 2, § 32 for a definition of the purpose of Part 2 of the Canadian Act. *See supra* text accompanying note 102.
209. *Id.* at pt. 2, § 31.
210. *Id.*
211. *Id.*
212. *Id.* at sched. 1, § 5.
213. *Id.* at sched. 1, § 4.7.2.
214. *See id.*
215. *Id.* at sched. 1, § 4.3.4.

The Act requires that information be protected no matter what method is used for storage.[216] The Canadian Act outlines the methods of protection including physical,[217] organizational,[218] and technological measures.[219] The Act does not give specifications for how the data should be technologically protected, but says that technological measures would include "the use of passwords and encryption."[220]

C. *United Kingdom*

The Data Protection Act in the United Kingdom is the statute responsible for the protection of personal information.[221] The Data Protection Act differentiates between personal data[222] and "sensitive personal data."[223] Part I

---

216. *See id.* at sched. 1, § 4.7.1. "The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held." *Id.*

217. *Id.* at sched. 1, § 4.7.3(a). Some examples of physical measures are "locked filing cabinets and restricted access to offices." *Id.*

218. *Id.* at sched. 1, § 4.7.3(b). Organizational measures could include: "security clearances and limiting access on a 'need-to-know' basis." *Id.*

219. *Id.* Encryption is "[t]he conversion of plaintext or data into unintelligible form by the means of a reversible translation, based on a translation table or algorithm. Also called enciphering." STALLINGS, *supra* note 15, at 377. A password is "[a] character string used to authenticate an identity. Knowledge of the password and its associated user ID is considered proof of authorization to use capabilities associated with the user ID." *Id.* at 378.

220. Personal Information Protection and Electronic Documents Act sched. 1, § 4.7.3(c).

221. *See generally* Data Protection Act, 1998, c. 29 (Eng.), See *supra* text accompanying note 108 for the purpose of the Data Protection Act.

222. *Id.* at pt. I, §1.

> In this Act, unless the context otherwise requires "data" means information which – (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should by means of such equipment, (c) is recorded as part of a relevant filing system, or (d) does not fall within paragraph (a) (b) or (c) but forms part of an accessible record as defined by section 68 . . . .

Id. Personal data is defined as:

> [D]ata which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Id. Sensitive Personal data is defined as:

> Personal data consisting of information as to – (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Unions and Labour Relations (Consolidations) Act 1992), (e) his physical or mental health condition, (f) his sexual life, (g) the commission or alleged commission by him of any offense, or (h) any proceeding fro any offense committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Id. at pt. I, § 2.

Schedule 2 outlines the protection of personal data.[224] Part I Schedule 3 outlines the protection of sensitive personal data.[225]

Part II of the Data Protection Act sets forth "the rights of data subjects and others."[226] It conveys the right of the individual to know whether information is being collected about them,[227] and if there is information being collected, they have the right to "be given by the data controller a description of (i) the personal data of which that individual is the data subject, (ii) the purpose for which they are being or are to be processed, and (iii) the recipients or classes of recipients to whom they are or may be disclosed . . . ."[228] Individuals have the right to the information, the source who supplied the data,[229] and the purpose of the collection of data.[230]

The individual is given the right to "prevent processing likely to cause damage or distress,"[231] the "right to prevent processing for purposes of direct marketing,"[232] and "rights in relation to automated decision-taking."[233]

---

223. *See id.* at pt. I, § 2; *see also supra* text accompanying note 222.
224. *See id.* at pt. I, sched. 2.
225. *See id.* at pt. I, sched. 3.
226. *Id.* at pt. II.
227. *See id.* at pt. II § 7(1)(a).
228. *Id.* at pt. II, § 7(b)(i)-(iii).
229. *Id.* at pt. II, § 7(c)(i)-(ii).
230. *Id.* at pt. II, § 7(d).

> [W]here the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in the decision-taking.

Id.

231. *Id.* at pt. II, § 10.

> [A]n individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing or processing for a specified purpose or in a specific manner, and personal data in respect of which he is the data subject, on the ground that for specified reasons – (a) the processing of those data or in that manner is causing or is likely to cause substantial damage or substantial distress to him or another and (b) that damage or distress is or would be unwarranted.

Id.

232. *Id.* at pt. II, § 11.

> (1) An individual is entitled at any time by notice in writing to a data controller to require the data controller to at the end of such period as is reasonable in the circumstances to cease, or not to begin processing for the purposes of direct marketing personal data in respect of which he is the data subject. (2) If the court is satisfied, on the application of any person who has given a notice under subsection (1), that the data controller has failed to comply with the notice, the court may order him to take such steps for complying with notice as the court thinks fit. (3) In this section "direct-marketing" means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.

Id.

Part IV provides the exemptions to the previous parts.[234] There are a number of exemptions including national security,[235] crime and taxation,[236] and "health, education and social work."[237] "The Secretary of State may by order exempt from the subject information provisions, or modify those provisions, in relation to, personal data consisting of information as to the physical or mental health condition of the data subject."[238]

The Data Protection Act is based on the European Union Directive 95/46/EC[239] of the European Parliament and of the Council of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[240] Section III defines special

---

233. *Id.* at pt. II, § 12. The individual can require that important decisions made about the individual are not made single-handedly by the automated processing of personal data. *See id.*

234. *See id.* at pt. IV.

235. *Id.* at pt. IV, § 28. "Personal Data are exempt from any of the provisions of - (a) the data protection principles, (b) Parts II, III, and V, and (c) section 55, if the exemption from that provision is required for the purpose of safeguarding national security." *Id.*

236. *Id.* at pt. IV, § 29.

> (1) Personal data processed for any of the following purposes - (a) the prevention or detection of crime, (b) the apprehension or prosecution of offenders, or (c) the assessment or collection of any tax or duty or of any imposition of a similar nature, are exempt from the first data protection principle.

Id.

237. *Id.* at pt. IV, § 30.

238. *Id.*

239. *See* Banisar, *supra* note 2, at 105; *see also* Council Directive 95/46/EC, 1995 O.J. (L 281) 31.

240. *See* Banisar, *supra* note 2, at 105. The following definitions are set forth in the Directive:

> (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more specific factors to his physical, physiological, mental, economic, cultural or social identity; (b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; (c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographic basis; (d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; (e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; (f) 'third party' shall mean and natural or legal person, public authority, agency or other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data; (g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed,

categories of data.[241] "Member states shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[242] The Act also provides for exceptions to this rule.[243]

> Paragraph 1 shall not apply where processing of the data is required for the purposes of preventative medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.[244]

Directive 95/46/EC also sets forth provisions for when the data should be given to the subject,[245] when the data subject has the "right of access,"[246] and when the data subject has the "right to object."[247] Additionally, Directive 95/46/EC addresses the "confidentially and security of processing," which is addressed below.[248]

VI. COMPLIANCE AND PENALTIES

A. *United States*

The Privacy Rule allows for the Secretary of Health and Human Services[249] to develop the policies and procedures for compliance.[250] There are two main principles for compliance, cooperation and assistance.[251] Individuals

---

> whether a third party or not; however, authorities which may receive data in a framework of a particular inquiry shall not be regarded as recipients; (h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to the personal data relating to him being processed.

Council Directive 95/46/EC, 1995 O.J. (L 281) 31, at ch. I, art. 2.

241. *See* Council Directive 95/46/EC, 1995 O.J. (L 281) 31, at ch. II, § III.

242. *Id.* at art. 8(1).

243. *See id.* at art. 8(3).

244. *Id.*

245. *Id.* § IV, art. 10.

246. *Id.* § IV, art. 12.

247. *Id.* § VII, art. 14. This section includes the subject's right to object and "automated individual decisions." *Id.* at § VII, art. 15.

248. *Id.* § VIII, art. 16-17. For more information about the security provisions see *infra* Part 4.

249. 45 C.F.R. § 160.103 (2003). "Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated." *Id.*

250. 45 C.F.R. § 160.304.

251. *Id.*

are given the right to file a complaint with the Secretary if they believe that a covered entity is noncompliant with the privacy provisions.[252] Once the Secretary receives the individual's complaint, he "may" investigate, and the investigation may "include a review of pertinent policies, procedures, or practices of the covered entity and of the circumstance regarding any alleged acts or omissions concerning compliance.[253] Additionally, the Secretary has the authority to perform compliance reviews.[254]

The Privacy Rule also sets out the responsibilities for covered entities to participate in compliance.[255] The Secretary is responsible for imposing mandatory penalties when organizations violate the statute.[256] However, the Secretary does have the exclusive authority to "settle any issue or case or to compromise any penalty."[257]

B. Canada

Division Two of the Canadian Act provides for complaints and remedies.[258] Under the Canadian Act an individual may file a complaint with

---

(a) Cooperation. The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance with the applicable requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter. b) Assistance. The Secretary may provide technical assistance to covered entities to help them comply voluntarily with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

Id.

252. 45 C.F.R. § 160.306. There are guidelines for how the complaint is to be filed. (b) Requirements for filing complaints. Complaints under this section must meet the following requirements: (1) A complaint must be filed in writing, either on paper or electronically. (2) A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter. (3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown. (4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

Id.

253. *Id.*

254. *See* 45 C.F.R. § 160.308.

255. 45 C.F.R. § 160.310. Covered entities are required to keep and provide records and compliance reports, cooperate with investigations and compliance reviews, and permit access to the information for investigation. *Id.*

256. 45 C.F.R. § 160.506 (2003). "The penalty imposed under §160.506 must be in accordance with 42 U.S.C. 1320d-5 [sic] and the applicable provisions of this part." 45 C.F.R. § 160.508 (2003).

257. 45 C.F.R. § 160.510 (2003). The exclusive authority is granted to the Secretary without or without the consent of the ALJ. 45 C.F.R. § 160.536 (2003).

258. Personal Information Protection and Electronic Document Act, R.S.C. ch. 5, at pt. 1,

the Commissioner regarding a violation of the provisions.[259] The Commissioner then determines whether "there are reasonable grounds to investigate" and subsequently "may initiate a complaint in respect of the matter."[260] Additionally, the Commissioner is required to notify the organization that there has been a complaint filed.[261] The Commissioner has the power to summon appearances, administer oaths, receive evidence, enter the dwelling of the organization at anytime, and examine and copy records in order to investigate the complaint.[262]

Following the investigation, the Commissioner has one year to make a report that includes: findings and recommendations, settlement by the parties, any request made by the organization, and any possible recourse.[263] The Commissioner's report is unnecessary in cases where the Commissioner finds that the complaint did not exhaust other reasonably available "grievance or review procedures," the complaint could be dealt with more appropriately by other laws of Canada, the elapsed time is "such that a report would not serve a useful purpose," or the complaint was "trivial, frivolous, or vexatious or is made in bad faith."[264] After the report is made, the complainant can request a hearing.[265] The available remedies include: an order to comply, an order for the organization "to publish a notice of any action taken or proposed to be taken to correct its practices," and "award damages to the complainant, including damages for any humiliation that the complainant has suffered."[266]

In addition, in order to ensure compliance, the Commissioner has the power to conduct audits if he reasonably believes there is a violation.[267] If the Commissioner finds it necessary, he may make public the personal information management practices.[268] The Canadian Act encourages witnesses to come forward with information by protecting their identity and prohibiting retribution against employees who come forward.[269] Individuals who intentionally violate the provisions are subject to fines up to $100,000.[270]

---

div. 2, § 11.

259. *Id.* at pt. 1, div. 2, § 11(1).
260. *Id.* at pt. 1, div. 2, § 11(2).
261. *Id.* at pt. 1, div. 2, § 11(4).
262. *Id.* at pt. 1, div. 2, § 12(1).
263. *Id.* at pt. 1, div. 2, § 13.
264. *Id.* at pt. 1, div. 2, § 13(2).
265. *Id.* at pt. 1, div. 2, § 14(1).
266. *Id.* at pt. 1, div. 2, § 16.
267. *Id.* at pt. 1, div. 3, § 18(1).
268. *Id.* at pt. 1, div. 3, § 20(2).
269. *See id.* at pt. 1, div. 4, § 27.
270. *See id.* at pt. 1, div. 4, § 28. The penalties range from "(a) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or (b) an indictable offence and liable to a fine not exceeding $100,000." *Id.*

C. *United Kingdom*

The focus of the European model is enforceability.[271] "The E.U. is concerned that data subjects have rights that are enshrined in explicit rules, and that data subjects can go to a person or an authority that can act on their behalf."[272] The Directive also requires information transferred out of Europe to be protected by similar laws, which has pressured other countries into developing laws to protect data.[273]

Council Directive 95/46/EC provides for the confidentiality of processing: "Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on the instructions from the controller, unless he is required to do so by law."[274] It gives guidelines for the processing of data.[275]

> Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data protected.[276]

In instances where the data controller is not doing the actual processing of the data, he is required to "choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with

---

271. *See* Banisar, *supra* note 2, at 12. "The key concept in the European model is 'enforceability.'" *Id.*

272. *Id.*

273. *See id.* at 12-13.

> This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. Those countries that refuse to adopt meaningful privacy law may find themselves unable to conduct transactions involving certain types of information flows with Europe, particularly if the transactions involve sensitive data.

Id. See also Council Directive 97/66/EC, art. 25.

274. Council Directive 95/46/EC, at § VIII, art 16.

275. *See id.* at art. 17.

276. *Id.* at art. 17, pt. 1.

those measures."[277] The Directive requires that the actions of the processor be governed by a contract.[278]

VII. PROBLEMS WITH PRIVACY AND SECURITY

A. *United States*

Despite all of the laws and regulations, many issues relating to the privacy and security of personal information in the United States continue.[279] It is difficult for the laws to keep up with technology.[280] When the laws are insufficient, enforcement remains at issue, and in some places the exemptions to the laws that are carved out for government agencies further decrease the protection.[281]

One growing problem is the amount of work involving electronic data that is done outside the United States.[282] For example, in the U.S. the "medical transcription industry is a $15 billion to $20 billion market."[283] There have been estimates that between four and ten percent of that work is subcontracted outside the United States to countries like Pakistan, India, China, and South Africa.[284] The problem arises out of the fact that HIPAA only applies to covered entities, so these subcontractors do not fall within the Act. Therefore, the Department of Health and Human Services cannot take action against these foreign entities.[285] Many of the hospitals do not even know the work is being done overseas until there is a problem.[286] This business practice threatens privacy.[287]

---

277. *Id.* at art. 17, pt. 2.

278. *Id.* at art. 17, pt. 3.

279. *See generally,* American Hospital Association, *Promises Under Pressure: HIPAA - Ensuring Privacy, Security & Administrative Simplification,* (2003 AHA Annual Membership Meeting paper), *available at* http://www.hospitalconnect.com (on file with author).

280. *Id.*

281. *See* Banisar, *supra* note 2, at 15.

282. *See* Tyler Chin, *Doctors Also Ship Work Overseas (But They Don't Always Know It) Offshore Outsourcing Can Save Physicians Money, But Can Also Present Potential HIPAA Problems,* http://www.ama-assn.org/amednews/2003/11/10/bisb1110.htm (Nov. 10, 2003) (last visited Oct. 11, 2004).

283. *Id.* This is according to the president of the American Association for Medical Transcription. *Id.*

284. *Id.* This outsourcing has been attributed to cost and the unavailability of qualified workers in the United States. *Id.*

285. *See id.* HIPAA does apply to the entities that hire the foreign contractors; however, there is no direct applicability to foreign companies. *Id.*

286. *See id.* Recently, a transcriptionist in Pakistan "threatened to post patient files on the Internet unless the University of California, San Francisco, Medical Center paid her money she claimed a third party owed her. . . . The women had been hired, through a series of subcontractors, to transcribe them." *Id.*

287. *See id.*

Legislation in the United States does not give specific guidelines for technical security.[288] "Generally speaking, the final security rules offer less detail and more generic guidance [than the proposed guidelines], in the sense of high-level direction, about how covered entities and their business associates should go about implementing security."[289] Therefore, the rules are principle-based rather than "checklists."[290] This means less of a risk for entities to comply with specifics; however, the rules could lead to more liability because they require entities to continuously monitor their security systems.[291]

Hospitals continue to take advantage of new technology by providing wireless internet for staff and patients, for example.[292] One survey found most are using some type of wireless technology.[293] However, wireless networks are notoriously insecure.[294] Although there are different systems for home and business wireless systems, a study found that many of the business systems were insecure, while some systems were not being used to their full security potentials.[295] This demonstrated that there is the need for a "wake up call to corporate IT departments" and "that the enterprise needs to be taking a more activist approach to wireless LAN security."[296]

Another major issue related to the use of wireless data deals with the laptops and handheld tools that hospital employees use to access wireless data.[297] When these devices are lost or stolen there is the potential for the finder to gain access to the information stored on them.[298] "Until such remote

---

288. *See* 45 C.F.R. § 164.304.

289. Richard D. Marks et al., *DWT Releases Analysis & Comments On HHS's Just-Released HIPPA Security Rules,* Davis Wright Tremaine LLP, Health Law Group Advisory Bulletin (Feb. 2003), http://www.dwt.com/practc/hc/_ecom/bulletins/02-03_HIPAASec Rules.htm [hereinafter *Analysis & Comments*].

290. *Id.*

291. *See id.*

292. *See* Bob Brewin, *Hospitalized? You Can Still Use Wi-Fi to Surf at Scripps Health,* Computerworld. *at* http://www.computerworld.com/industrytopics/healthcare/story/0,10801, 86167,00.html (Oct. 17, 2003) (last visited Nov. 19, 2003). Scripps Health claims to be using a system that allows them to "segment public traffic from the operational network" *Id.*

293. *See* Randy Gainer et. al., *No Rest for the Wary, at* http://www.dwt.com/ practc/hc_eecom/bulletins/05-03_BNAarticle.htm (n.d.) (last visited Nov. 19, 2003); *see also* The Healthcare Information and Management Systems Society (HIMSS), *Leadership Survey* (Feb. 23, 2004), http://www.himss.org/2003survey/ASP/healthcarecio_home.asp (last visited Nov. 19, 2003).

294. *See* Bob Brewin, *Worldwide 'War Drive' Exposes Insecure Wireless LANs,* Computerworld, *at* http://www.computerworld.com/mobiletopics/mobile/story/0,10801, 74103,00.html (Sept. 9, 2002) (last visited Nov. 23, 2003) [hereinafter *Worldwide War Drive*]. One of the inherent flaws in wireless internet technology is the fact that data is transmitted via radio waves which are emitted outside of buildings allowing outsiders to catch the signals. *See* Gainer, *supra* note 293. Additionally, that data is typically not well protected so hackers are able to access it. *See id.*

295. *See Worldwide War Drive, supra* note 294.

296. *Id.*

297. *See* Gainer, *supra* note 293.

298. *See id.*

destruction of data moves from 'Mission Impossible' fiction to become commercially available on laptops and PDAs, IT administrators and privacy officers need to plan how they will minimize access to protected health information on lost and stolen portable wireless devices." [299] Hospitals may consider following the Department of Defense, which banned the use of wireless communications due to poor security.[300]

Additionally, the financial impact of the regulations will be significant.[301] The cost to become HIPAA compliant has been estimated to be greater than three billion dollars nationwide.[302] This will have an impact on state and local governments as well as private industry.[303] The Final Rule provides more flexibility by recognizing the significant costs of the regulations.[304] The healthcare industry in the United States is a 1.3 trillion dollar industry; thus, regulations will have a significant impact on the industry.[305] However, some of the regulations requiring electronic claim submissions could potentially save money.[306]

One attorney predicts that the litigation could be "as lucrative as asbestos and breast implant litigation combined."[307] The way the statutes are worded the encryption of data is addressable, not required, and provisions like this could

---

299. *Id.*

300. *See id. See also* Ellen Messmer, *Pentagon Prohibits Wireless, Citing Security Reasons,* Network World Fusion (Sept. 27, 2002), http://www.nwfusion.com/news/2002/0927pgon.html (last visited Nov. 19, 2003). "Given the exploitable vulnerabilities inherent in current wireless products and technologies and the interdependence of Defense and Pentagon networks, it is essential and expected that all tenants will strictly adhere to this policy." Memorandum from Howard G. Becker, Acting Director, Admission & Management, & John P. Stenbit, Assistant Secretary of Defense/DoD Chief Information Officer, to Secretaries of Military Departments, Pentagon Area Common Information Technology (IT) Wireless Security Policy (Sept. 25, 2002).

301. *See* Bob Berwin, *New HIPAA Security Rules Could Open Door to Litigation,* Computerworld, *at* http://www.computerworld.com/securitytopics/security/story/0,10801,78684,00.html (Feb. 20, 2003) (last visited Nov. 23, 2003) [hereinafter *Door to Litigation*].

302. Dibya Sarkar, *HIPAA Could Mean Big Business,* Federal Computer Week, *at* http://www.fcw.com/geb/articles/2002/0715/web-hipaa-07-19-02.asp (July 19, 2002) (last visited Oct. 11, 2004).

303. *See id.* "[S]tate and local governments and other groups have complained that the deadlines are too stringent and the issue too complex. Many want more time and guidance from the federal government. The federal government has offered some extensions." *Id.*

304. *See Analysis & Comments, supra* note 289. This provides a substantial benefit to small and rural providers. *See id.* Nevertheless it does not mean they do not need to comply with the regulations. *See id.*

305. *Door to Litigation, supra* note 301.

306. Richard D. Marks, *Surviving Standard Transactions: A HIPAA Roadmap,* 8 BNA'S ELECTRONIC COMMERCE & L.R. 22 (June 4, 2003), http://www.dwt.com/practc/hc_ecom/publications/06-03_BNA.htm [hereinafter *HIPAA Roadmap*]. For example, electronic claims submission costs anywhere between twenty-five and seventy-five cents, where the traditional paper filing costs between $2 and $12 per claim. *Id.*

307. *Door to Litigation, supra* note 301.

leave some information unprotected.[308] The interpretation and "risk analysis" will have a huge impact on the efficacy of the security rule.[309]

B. Canada

The New Canadian regulations got off to a rough start when the Information Commissioner resigned in 2003.[310] The timing of the resignation may have had a detrimental effect because it is said to have "created uncertainty at a time when, more than ever, new federal rules on privacy protection need to be promoted, interpreted and enforced."[311] One of the key problems that resulted from the change in the Commissioner is the uncertainty and the immediate need for interpretation.[312]

A major criticism of the Canadian Act is that the codes are vague due to their "multi-sectoral" nature.[313] The generality may cause difficulties when it comes to enforcement of the legislation.[314] This generality leads to a certain degree of uncertainty when it comes to what organizations are required to do and what is actually protected.[315]

One major issue is whether there is an objective standard. "For example, an organization is required to make a 'reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.'"[316] This may not be possible if the information is being collected online because of the various ways to access web pages, and it has not yet been determined whether posting the purpose for which the information will be used on a web page would be considered a "reasonable effort."[317] The Act has also been criticized because, while the legislation refers to the "reasonable individual," there is no clear definition of what the "reasonable individual" is, and consumers and businesses would view the standard differently. As such, it is unclear and ambiguous.[318]

Another criticism of the Canadian Act is that it does not specifically define which information is sensitive.[319] The Act states that, "in determining the form of consent to use, organizations shall take into account the sensitivity

308. *See id.*
309. *See id.*
310. *See* Tyler Hamilton, *Radwanski's Departure Comes at a Critical Stage*, TORONTO STAR, June 25, 2003.
311. *Id.*
312. *See id.*
313. *See* Teressa Scassa, *Making Sense of Canada's New Personal Information Protection Legislation*, 32 OTTAWA L. REV. 1, 3 (2000/2001).
314. *See id.*
315. *See id.*
316. *Id.* at 10.
317. *See id.*
318. *See id.* at 11.
319. *See id.* at 12-13.

of the information."[320] This could lead to high levels of privacy invasion when it comes to information that is considered less sensitive.[321] When compared to the European Directive 95/46/EC, the Canadian Act gives little guidance as to what information is highly sensitive, whereas the European Directive spells out what information cannot be processed.[322]

Another complaint of the Canadian Act is the lack of a provision for input from the public.[323] The role of the Privacy Commissioner is to disseminate information to the public but there is no outlet for public complaints about the regulations.[324] The majority of information available does not reflect the views of the people in relation to the privacy of their health information.[325] Most of the information available on the "ethics, management, and legality of sharing personal information is written from the perspective of health professionals legal experts and social service workers."[326] This problem of "lack of understanding of the 'popular will' in relation to the interprofessional exchange of personal health information lies in the conduct of properly formulated research on the issue."[327]

As the Canadian Act continues to come into effect there are a number of likely issues that will arise.[328] The role of the Privacy Commissioner will have a significant impact on how the legislation plays out and the development of the reasonable individual standard will determine what is actually protected.[329]

C. United Kingdom

There has also been much discussion about the Data Protection Act. In a compliance report regarding websites, it was noted that smaller institutions have more difficulty understanding the Data Protection Act as well as complying with it.[330] This may be due to the fact that the larger organizations can communicate directly with the Information Commissioner[331] where the smaller organizations cannot.[332] Additionally, the smaller organizations cannot

320. Personal Information Protection and Electronic Documents Act, R.S.C. ch. 5, at pt. 4.3.2.

321. Scassa, *supra* note 313, at 12.

322. *See id.* at 13.

323. *See id.* at 19-20.

324. *See id.*

325. Weitz et al., *supra* note 32.

326. *Id.*

327. *Id.*

328. *Id.*

329. *See id.*

330. *See* UMIST AND THE OFFICE OF THE INFORMATION COMMISSIONER, STUDY OF COMPLIANCE WITH THE DATA PROTECTION ACT 1998 BY UK BASED WEBSITES 24 (2002) [hereinafter STUDY OF COMPLIANCE].

331. *See id.*

332. *See id.*

afford the legal advice.[333] The larger corporations have noted that it is taking increased time to communicate with the Commissioners office.[334] The smaller companies are also concerned with poor communication and the fear that they will not be made aware of changes to the Act.[335]

In addition to the need for additional communication, there is a need for education of smaller companies.[336] Currently, some concerns with education are the costs and the lack of "Frameworks for Compliance."[337] For example, "if you are a small shop who collects credit card information for your own purposes you should comply in the following way . . . if you are a travel agent . . . who passes the information to others[,] e.g.[,] to an airline or hotel[,] then you should comply in the following way."[338]

This lack of clear definitions was apparent in the 2000 Source Informatics[339] case where the court determined that Directive 95/46/EC did not prevent the anonymisation of personal data that could then be disclosed and the court did not analyze how the process would have been interpreted under the Data Protection Act.[340] Critics of the decisions argue that there was "no basis for this assumption: it was merely asserted that 'common sense and justice' leads to the conclusion."[341] This demonstrates that although the Data Protection Act was effective at the time of the Source Informatics decision, the court did not look to its provisions.[342] However, a strict reading of the principles could lead to a stifling of legitimate research based on the fear of legal consequences.[343]

There is also a lack of certification process.[344] There are different claims of certification being used on websites in the United Kingdom, but there is no certification process that determines whether a site is "data protection compliant."[345] Moreover, the Information Commission has reported that there are "bogus agencies" claiming to be the Information Commission and falsely notifying businesses of violations.[346] The Commission recommends not immediately sending money and confirming that the correspondence is truly

333. *See id.* at 24-25.
334. *See id.* at 25.
335. *See id.* at 25.
336. *See id.*
337. *Id.*
338. *Id.*
339. *See* R. v. Department of Health, ex parte Source Informatics, 1 All E.R. 786 (2000).
340. *United Kingdom – R. v. Department of Health Ex Parte Source Informatics*, 8 MED. L. REV. 115 (Mar. 2000).
341. *Id.*
342. *See id.*
343. *See* Ian Walden, *Anonymising Personal Data,* 10 INT'L J. L. & IT 224 (2000).
344. *See* STUDY OF COMPLIANCE, *supra* note 330.
345. *See id.*
346. *See* Information Commissioner's Office, *Bogus Agencies, at* http://www.informationcommissioner.gov.uk/eventual.aspx?id=3677 (n.d.) (last visited Oct. 30, 2004).

from the Office of the Information Commissioner before responding.[347]

Lastly, there has been criticism that the EU Directive will make it difficult to do business with other countries.[348] On July 27, 2003, the European Commission "adopted a 'Decision' approving the US [sic] 'safe harbor' arrangement."[349] This is set up to give U.S. organizations standards to comply with in order to do business with E.U. members.[350]

VIII. CONCLUSION

In general, the problem of the privacy of personal medical information is worldwide.[351] Countries around the world are attempting to create legislation that will find a balance between efficient and effective health care systems and maintaining patient privacy.[352] There are different ways to attack the problem including comprehensive and sectoral laws and combinations of the systems.[353]

One of the common underlying problems with the privacy regulations in the United States, Canada, and the United Kingdom is the lack of technological specifications, which allows for a high degree of ambiguity within the regulations. Additionally, there appears to be a common concern regarding the amount of money that will be needed to comply with the regulations. Nevertheless, across the board, there is a serious effort to ensure the privacy of public health data.[354]

The United States, Canada, and the United Kingdom all address differently which information is included.[355] The sectoral laws in the United States include specifically what information is covered;[356] the comprehensive laws in the United Kingdom also explicitly state the categories of information that deserve special attention.[357] However the comprehensive laws in Canada do not define what information is "sensitive," leaving more ambiguity than in

---

347. *See id.*

348. *See* Banisir, *supra* note 2, at 12-13. *See also* text accompanying note 273.

349. *See* Information Commisioner's Office, *US Safe Harbour, at* http://www.informationcommissioner.gov.uk (n.d.) (last visited Oct. 30, 2004) [herinafter *US Safe Harbour*]; *see also* U.S. Department of Commerce, *Safe Harbour, at* http://www.export.gov/safeharbor/ (last updated June 29, 2004).

350. *US Safe Harbour,.supra* note 349.

> The scheme will involve organizations in the States committing themselves to comply with a set of data protection principles backed up by guidance provided through a number of 'frequently asked questions.' Commitment to 'safe harbours' will provide an adequate level of protection for transfers of personal data to the US from EU Member States.

Id.

351. *See supra* Part II.

352. *See supra* Part IV.

353. *See id.*

354. *See id.*

355. *See generally, supra* Part V.

356. *See generally, supra* Part VI.

357. *See id.*

the other regulations.[358] Only time will truly tell which regulations are effective, and what needs to change. Nevertheless, this will continue to be an important area to watch internationally.

358. *See id.*

> Since consent is supposed to be given for particular uses, the degree of consent required should not be tied specifically to the nature of the information. This is certainly the approach in the Quebec legislation which requires 'manifest, free and enlightened' consent regardless of the circumstances. The linking of the form of consent to the nature of the information in *PIPA* is a further indication of the weakness and ambiguity of the consent principle. Needless to say, it also gives rise to further problems of interpretation.

Scassa, *supra* note 313, at 12.